REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **12 06 2009**	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* 21-07-2008 to 12-06-2009

4. TITLE AND SUBTITLE **ISLAMIC EXTREMISTS LOVE THE INTERNET**	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Lieutenant Colonel Donald P. Taylor, II, United States Army	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd. Norfolk, VA 23511-1702	**8. PERFORMING ORGANIZATION REPORT NUMBER** JFSC 25789
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Al-Qaeda and its network of followers have had great success during this decade with their efforts to influence the West. Which cyber tool have these terrorists used as their main weapon to achieve their objectives? What effect is this having on America's younger generation? Since September 11, 2001 Islamic extremist terrorists have been exploiting the Internet to promote their radical ideology and today they are targeting select youth, developing them into home-grown terrorists who support their cause. A careful study of select terror Web sites reflects that jihadists are promoting their propaganda and highlighting successful operations directed against our government and the US military. What cyber techniques are being used for persuasion? How are our leaders handling this threat? Is there more they can be doing? This author's thesis is that Islamic extremists are exploiting the Internet resulting in the development of home-grown terrorists a serious vulnerability which the US government has inadequately addressed.

How does this threat impact the Department of Defense and the combat commander's mission? This premise illustrates how the terrorists are gathering sensitive information, occasionally critical information, and valuable data points from the Internet and using these resources to construct combat operational planning directed against our forces. Operational security education is paramount for all department employees and military commands. This paper illustrates the OPSEC process. It also recommends a strategic counter-strategy to the extremists' Web site influence.

15. SUBJECT TERMS
Terrorists, Internet, Operational Security (OPSEC), Potential Home-Grown Terrorists

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ms. Stacey Newman
a.	**b. ABSTRACT** **Unclassified**	**c. THIS PAGE** **Unclassified**	Unclassified Unlimited	80	**19b. TELEPHONE NUMBER** *(include area code)* 757-443-6301

JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL

ISLAMIC EXTREMISTS LOVE THE INTERNET

By

Donald P. Taylor, II

Lieutenant Colonel, USA

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of the Defense.

Signature_________________________

03 April 2009

Thesis Advisor: Dr. Vardell Nesmith, JFSC

Abstract

Al-Qaeda and its network of followers have had great success during this decade with their efforts to influence the West. Which cyber tool have these terrorists used as their main weapon to achieve their objectives? What effect is this having on America's younger generation? Since September 11, 2001 Islamic extremist terrorists have been exploiting the Internet to promote their radical ideology and today they are targeting select youth, developing them into home-grown terrorists who support their cause. A careful study of select terror Web sites reflects that jihadists are promoting their propaganda and highlighting successful operations directed against our government and the US military. What cyber techniques are being used for persuasion? How are our leaders handling this threat? Is there more they can be doing? This author's thesis is that Islamic extremists are exploiting the Internet resulting in the development of homegrown terrorists a serious vulnerability which the US government has inadequately addressed.

How does this threat impact the Department of Defense and the combat commander's mission? This premise illustrates how the terrorists are gathering sensitive information, occasionally critical information, and valuable data points from the Internet and using these resources to construct combat operational planning directed against our forces. Operational security education is paramount for all department employees and military commands. This paper illustrates the OPSEC process. It also recommends a strategic counter-strategy to the extremists' Web site influence.

Table of Contents

List of Figures

I. Introduction.

Since September 11, 2001 Islamic extremists have been exploiting the Internet to promote their radical ideology and today they are targeting select youth, developing them into home-grown terrorists supporting their cause. Some combat commanders may not grasp the Internet's security consequences or its cause and effect on those under their command. These terrorists fully understand the ubiquitous nature of the World Wide Web because the Internet provides freedom of speech for them, which in-turn becomes a tool for mass communication perception management. Al-Qaeda (AQ) has manipulated the Internet in order to disseminate their philosophy and propaganda. Likewise, they have used it to provide operational direction for their irregular warfare directed against the West.[1] Furthermore, research on this subject has shown that the US Government does not know how to effectively counter this strategic menace through the employment of the informational element of national power.

Secretary Robert Gates alluded to this notion when he addressed the National Defense University students in the fall last year on his National Defense Strategy for 2008, stating that our enemies were exploiting the Internet. He referred to the extremists' skillful use of the Internet in Iraq and Afghanistan in order to spread their propaganda, and intimidate the local populations. He also deplored the U.S. government's bounds in this area.[2]

[1] Bruce Hoffman of the RAND Corporation, "*Testimony- The Use of the Internet by Islamic Extremists*," presented to the House Permanent Select Committee on Intel (May 04, 2006): 4.

[2] Secretary Gates visited the National Defense University on 29 September 2008 and at 1000 hours addressed the students and faculty on his 2008 National Defense Strategy via VTC

The extremists' manipulation of the Internet has been more prevalent in Iraq vice Afghanistan. However, as of late February 2009 reports indicate that instructional suicide bomber videos are increasingly coming out of Afghanistan. Secretary Gates' reference also reinforced his notion of AQ being better at communicating its message on the Internet than America in late 2007.[3] Furthermore, this menace is not just a focus for the Iraq and Afghanistan theaters of operation, but it is also of a grave concern for our nation's homeland security and safety. Even the U.S Department of State recognizes that terrorists are exploiting the Internet's infrastructure for a multitude of purposes to further their ideological cause.[4]

For the past seven years, Al-Qaeda (known as "The Base") has been extremely competent at exploiting the Internet in order to influence both civilian and military audiences for their own agitprop purposes. Yet, today they are not the only terrorist group taking advantage of this electronic communications network. Different Islamic extremist terrorist groups, such as Hamas and Hezbollah, mimic their style of using the Internet but for this study's purpose AQ will be the primary focus since they are the model others are emulating. Hamas, Hezbollah, and other extremist web site activity will be referred to in the next chapter.

[3] The Moderate Voice, Secretary Gates: "Al Qaeda is better at communicating its message on the Internet than America, November 27, 2007: as quoted by NY Times", http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-0.87603.3513028242.html (accessed September 26, 2008)

[4] U.S Dept of State, released by the Office of the Coord for CT. "Country Reports on Terrorism, April 28, 2006", http://www.state.gov/s/ct/rls/crt/2005/64333.htm (accessed October 7, 2008

Our nation’s leaders need to be concerned about how Islamic extremists can influence their strategic objectives through the use of the Internet. The terrorists have the ability to communicate in real time via the enticing virtual world of the Web, which includes dramatic video footage, still photographs, and influential audio clips.[5] The terrorists’ capacity to do this enables them to reach the masses extremely quickly and have a major influence, especially on the younger generation.

This thesis will illustrate how Islamic extremists are exploiting the Internet and using it as a tool for their radicalization movement. As a result, select youth are influenced, resulting in occasional potential home-grown terrorists. It will attempt to explain and illustrate “how violent Islamic terrorist groups like AQ are using the Internet for communication purposes, to enlist followers into the global Islamic terrorist movement and to increase support for their movement, ranging from ideological support, to fundraising, and ultimately to planning and executing terrorist attacks.”[6] The paper will document the history of how the Internet has advanced the Islamic extremist’s ideology and how it has affected our society today. For the semantic purpose of this paper, the terms terrorists and extremists are used interchangeably for radical Islamic identification.

[5] Gabriel Weimann, “Terror on the Internet: The New Agenda, The New Challenges,” Seminar Held at the United States Institute of Peace, Washington D.C., April 10, 2006.

[6] Report source 8 May 2008, United States Senate Committee on Homeland Security and Governmental Affairs.

This author's thesis is that Islamic extremists are exploiting the Internet resulting in the development of home-grown' terrorists, a serious vulnerability which the US government has inadequately addressed.

Sun Tzu, the famous 6th Century B.C. Chinese military strategist wrote, "If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril."[7] His 2,600 year old military maxim is as relevant today as it was then. If we remain ignorant of our adversary's Internet exploitation, do not fully comprehend this threat and respond appropriately soon, it is highly likely that this will get well beyond our operational control and have severe strategic consequences for this nation's next generation of disgruntled youth. Hopefully, this research paper will bring to the reader's attention that Islamic extremists are exploiting the Internet to their advantage and how the average common computer user is unknowingly assisting that exploitation due to a lack of operational security awareness. A further point will be made in the illustration of future networks in social networking that have the potential for Islamic extremist terrorists' exploitation that may affect their Intel collection, recruitment, propaganda efforts, and command and control aspects. Finally, after a thorough analysis of the topic the author will conclude with a proposal focusing on the informational element of national power that will assist in mitigating the effect that the Internet is having on those potentially influenced individuals.

[7] Samuel Griffith, Sun Tzu: The Art of War (New York: Oxford University Press, 1971), 84.

II. Terrorists' Use of the Internet.

History of the Extremists' Web Sites

The Internet enabled AQ to bring upon this nation the September 11, 2001 cataclysmic event that has for ever changed our lives, and it really came to fruition after the Al-Qaeda fighters scattered following the US invasion of Afghanistan. The Jane's Terrorism and Insurgency Center's November 2001 review documented that the "19 hijackers were linked together through the Internet with their communications, banking transactions, hotel and rental car reservations, pilot training, and purchasing of their airline tickets"[1] in preparation for that fateful morning. Yet, on the morning after the attack on the Twin Towers you could still visit a Web site that integrated three of the wonders of technology: the Internet, digital video, and the World Trade Center.[2]

Even the 9/11 Commission Report cites four specific instances in which the "19 hijackers accessed information from the Internet to plan or facilitate the 9/11 attacks."[3] Right after the attacks on the towers, several Internet Web sites permitted users worldwide to cherish what millions of tourists have delighted in since the architectural wonder was completed in 1973: the glorious forty-five mile view from the top of the World Trade Center. According to journalists, the caption on the sites still read "Real-Time Hudson River View From World Trade

[1] Periodical, Jane's review, 01 Nov 2001, "What the Investigation Reveals", http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed 14 Sep 2008)

[2] Maura Conway, "Reality Bytes," *Cyberterrorism and Terrorist Use of the Internet" (July 2005):5.* http//www.firstmonday.org/ISSUES/issue7-11/conway.html (accessed 10 October 2008)

[3] Final Report of the National Commission on Terrorist Attacks Upon the United States. The *9/11 Commission Report: Authorized Edition* (New York & London, W.W. Norton & Company, 2004), pp. 157, 164, &495.

Center."[4] A short time afterwards, the square in the ground from space was a deep black nothingness from where the buildings once stood.

When terror struck the homeland at that point, it was played for individuals over and over on a vast network of computers sites, reinforcing our vulnerability. Just to reflect on the rapid growth of the extremist cyber network, fourteen years ago there were only "around 12 terrorist-related Web sites and by 2006 that multiplied to more than 5,000."[5] As of 2009, this author estimates that there are more than 6,200 of these sites considering the 400% increase between 1995 and 2006; however, it is difficult to prove an exact number because these sites are continually appearing and disappearing at random.

In a span of three decades, the Internet has morphed from a U.S. Department of Defense (DoD) command and control network, consisting of less than one hundred computers to a network that criss-crosses the globe.[6] Today, the Internet is made up of tens of thousands of nodes (i.e., linkage points) with more than 105 million hosts spanning more than 200 countries. With an estimated population of regular users to be more than six hundred million people, the Internet has become a near-universal presence in many world regions. That ubiquity is due in large part to the release in 1991 of the World Wide Web. In

[4] Armistead, E. Leigh and Dr. Maura Conway. Information Warfare, Separating Hype From Reality: Cyberterrorism, Hype and Reality, (Virginia, Potomac Books, 2007), 94.
[5] Capital Hill Hearing Testimony, "Internet and Terrorism", 6 Nov 2007, http://psidonline.isr.umich.edu/Publications/Congressional_Testimony.pdf, (accessed 26 Sep 2008)
[6] Armistead, E. Leigh and Dr. Maura Conway. Information Warfare, Separating Hype From Reality: Cyberterrorism, Hype and Reality, (Virginia, Potomac Books, 2007), 91.

1993, the Web consisted of a mere 130 sites, by century's end it boasted more than one billion.[7]

Jihad Spreading on the Internet.

Our enemies understand how to promote and direct their jihad (Islamic religion holy war) at the Western world through the Internet, and they realize how it has become an extensively integrated part of life for our culture. Al-Qaeda and their Islamic extremist followers have become the first irregular movement in history to migrate from the physical space to cyberspace, inspiring radicalized Muslims worldwide to join their jihad." The virtues of the Internet are: the ease of access, the lack of regulation, the vast potential audiences, and the fast flow of information has assisted the extremists in achieving their ideological goals."[8] The World Wide Web enables these individuals to do this at any time of their choosing, day or night. Through this communicative network, the Internet has enabled its participants to contribute in open forums and discuss pertinent matters concerning the jihad.

Pursuant to this jihad, a list of U.S. Department of State's Foreign Terrorist Organizations (FTO) dated as of 2005 reflected 42 different terrorist organizations, all of which are affiliated with Islamic extremism and have an affiliated Web site.[9]

[7] Armistead, E. Leigh and Dr. Maura Conway. Information Warfare, Separating Hype From Reality: Cyberterrorism, Hype and Reality, (Virginia, Potomac Books, 2007), 92.

[8] "How Terrorists Use the Internet": 7.62mm Justice, by Howard Salter and quoted from Gabraen, 05 Nov 2007, http://762justice.com/2007/11/05/how-terrorists-use-the-internet/, (accessed 30 Aug 2008)

[9] U.S DOS Fact Sheet, Office of Counterterrorism- October 11, 2005, Foreign Terrorist Organizations (FTOs), http://www.state.gov/s/ct/rls/fs/37191.html (accessed October 27, 2008)

The previous FTO list published in December 2001 had 105 terrorist organizations, but not all of them were related to Islamic extremism, nor did they all own a Web site.[10] This report trend seems to be that an FTO list is released about every four years and the DOS' FTO list due out for 2009 is yet to be published.

Research shows that AQ and its followers are becoming even more sophisticated in the use of the Internet, which is resulting in an infallible means to carry out destructive operations. It appears that the terrorists have designed an operational technique around the Internet idea of multi-national communication links. The genesis of this effort is the main "spread of radical Salafi Internet sites that provide religious justification for the attacks"[11] and in the past, our nation has not been paying a great deal of attention to it. Even the former president's Critical Infrastructure Protection Board Chief of Staff recognized that they "were not understanding the amount of attention Al-Qaeda was paying to the Internet"[12] in 2002. Now, at least Congress seems to have an interest in the threat it poses, considering the recent congressional testimonies chaired by Senator Joseph Lieberman.

This paper's investigation indicates that prior to 9/11, AQ solicited people with computer skills who could assist with Osama Bin Laden's vision of a global

[10] U.S DOS Chronology, The Office of the Coordinator for Counterterrorism- December 31, 2001, Identified Terrorist Groups, http://www.state.gov/s/ct/rls/fs/2001/6531.html (accessed October 7, 2008)

[11] The Jawa Report, "The Threat of Home-grown Terrorists is Real", 6 Feb 2008, http://mypetjawa.mu.nu/archives/191108.php, (accessed 29 Sep 2008)

[12] Washington Post, "Terrorists at the Threshold of Using Internet as Tool of Bloodshed", June 27, 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html, (accessed 26 Sep 2008)

crusade, which led to those horrendous attacks on our homeland. But this did not come without an initial trepidation from his followers. During this timeframe, Islamic extremists and the jihadist networks were conducting internal discussions. These sometimes resulted in heated debates over the issue of the Internet activism and whether it was even harmonious with Islamic law and its traditions.[13]

Some even argued that the Internet was a 'Jewish conspiracy' but the end result was that it quickly became a cyber-weapon in the hands of terrorists. As a result of this dispute, "Al-Qaeda has long had a media committee"[14] and during the course of this era it operated the www.alneda.com Web site right up to the fall of 2005, when it eventually disappeared. This Web site advertised the core terrorist enlistment message and disseminated official statements from AQ under the leadership of Yusuf Salih Fahad al-Ayiri.[15] This site was established and distributed globally, via the web addresses of many Internet Service Providers (ISP) before the 9/11 attacks and was AQ's first Web site. Al-Ayiri intended for 'mirror' sites to be activated whenever one ISP would close down therefore maintaining its integrity.[16]

Al-Qaeda's Alneda Web site, which was presented only in the Arabic language when it was active, emphasized four core messages that remain the basic staple of AQ and other jihadi Web sites today. First, it stated that the West has a

[13] Jane's Terrorism and Insurgency Center, Information Campaigns, pg 6- August 01, 2007, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)
[14] The 9/11Commission Report, p.145, released 22 July 2004
[15] Jane's Terrorism and Insurgency Center, Information Campaigns, pg 6- August 01, 2007, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)
[16] Jane's Terrorism and Insurgency Center, Information Campaigns, pg 7

relentless hostility towards Islam. Second, violence is the only answer to address this threat and the West understands this. Third, jihad is the only true option to counter this. The last message was that Muslims must recognize the alleged control, suppression, and censorship of information about the jihadi struggle by the West and established media outlets.[17]

This evidence points to the presumption that Bin Laden saw the potential of the Internet for fund raising and publicizing his cause early-on. Moreover, during the early 1980's, bin Laden had recruited Egyptian computer experts to create an extensive network of Web sites, e-mail capabilities, and electronic bulletin boards that continue to function today.[18] Bin Laden has also long understood the Internet's capability of providing three critical functions for AQ:

1. Its propaganda potential for recruitment, fund raising, and ability to shape public opinion in the Muslim world;

2. Terrorist' training and instruction through the virtual world; and

3. Its operational planning potential for attacks through both e-mail communication and the access provided from useful Open Source Information (OSINT).[19]

[17] Jane's Terrorism and Insurgency Center, Information Campaigns, pg 9

[18] Hoffman, Bruce of the RAND Corporation, "*Testimony- The Use of the Internet by Islamic Extremists*," 6.

[19] Hoffman, Bruce of the RAND Corporation, "*Testimony- The Use of the Internet by Islamic Extremists*," 8.

Terrorists' Understanding of the Internet's Importance

Al-Qaeda understands that the Internet is a global scale "virtual sanctuary" and it is anonymous but pervasive.[20] Basically what this means is that it enables the terrorists to operate in a universal computer network refuge that lacks any individual recognition of who is on the keyboard. The development of the computer has enabled the Islamic radical to perform pertinent Internet actions, which include the use of e-mail, and the ability to congregate in chat rooms and carry on discussions on network bulletin boards. The Internet has also enabled the development of terrorists' web sites, the promotion of graphic videos, the opportunity to raises funds to finance their activities, and the posting of blogs. Blogs will be discussed in the next chapter. The extremists have used all of these communication tools to promote their propaganda.[21]

These multiple communication means are enabling our adversaries to collect intelligence on the Department of Defense (DoD). An example of this would be for our enemies using the government google search engine to locate just about anything they wanted concerning the DoD on the open net. Furthermore, the Internet allows terrorists to coordinate their actions, educate and train their followers on either ideology or jihad. They are also able to indoctrinate and recruit others through the spread of their propaganda message, and raise funds to finance their activities. These Internet means offer terrorists a number of advantages over more traditional communication. It is easy to operate and access,

[20] Agence France Presse- English, Weakened Military, "*Al-Qaeda Fights On-line*", http://resources.bnet.com/topic/al-qaeda+and+civilian.html, (19 Feb 2007)
[21] Agence France Presse, *Al-Qaeda Fights On-line*, 2.

due to little or no government control, and it has the ability to reach enormous and foreign audiences simultaneously.[22]

But when the extremist Web sites have been identified, hacked, or shut down by Internet Service Providers, the terrorists have turned to chat rooms and message boards for communication. Terrorists know this vast media network provides a tremendous speed of communication and global linkage that enables them to successfully organize their disruptive and deadly activities. It has been known for some time that bin Laden and the Islamic extremists are skillful at using advanced technologies on the Internet.[23]

Matt Devost of the Terrorist Research Center points out that AQ and its associates have used these technologies including encryption programs that are free on the Web, as well as more powerful anti-spy software purchased on the open market.[24] The term used to describe this coded technique for their operational communication is called steganography and it is widely used by them. The terrorists tend to operate in secrecy on the "Web while organizing, scheduling and conducting meetings that are used mostly for propaganda development and information exchange."[25] Steganography is defined as the practice of concealing a message, image, or file and the terrorists do this by inserting them on the Web into electronic files. Another term to describe this is cryptography. Our

[22] Hoffman, "*Testimony- The Use of the Internet by Islamic Extremists"*, 1.
[23] Hoffman, "*Testimony- The Use of the Internet by Islamic Extremists"*, 3.
[24], NewsFactor Network- "How the Terrorists Use the Internet", by Matthew Devost from the Terrorist Research Center)- 12 sep 2001, http://www.newsfactor.com/perl/story/7731.html, (accessed 14 September 2008)
[25] NewsFactor Network- "How the Terrorists Use the Internet", 2

adversaries are so adept at this that the average person, while on the Internet does not even know the hidden messages are there. Terrorists have been suspected of hiding pictures and maps of targets in seemingly innocent chat rooms and various Internet bulletin boards.

Mr. Devost's reference to how terrorists are exploiting the Internet substantiate the first portion of this author's thesis statement. He goes on to mention that the Web gives terrorists the potential to target the economy, power, transportation, and other systems that rely on information that is linked to the network..[26] Even though his thinking is over eight years old, in deference to Mr. Devost, it seems unlikely that the terrorists would use the Internet as a weapon to attack our country, but rather use it as a means to exploit and further their ideological goals just as they are currently doing.

Our government has specialized organizations that are monitoring this activity and they need to continue to do so. But the future generation of Islamic extremist terrorists bent on waging their jihad will manipulate the Internet to even greater measures than those of the past through social networking and new applications for spreading ideology.[27] This in-turn will undoubtedly result in our government having an increased difficulty in detecting their attempts especially with the multiple means of application available to them.

[26] NewsFactor Network- "How the Terrorists Use the Internet", 4

[27] "Al Qaeda Beats the Odds; Terror Network Uses the Gambling Web sites to Launder Money in Internet Campaign", January 03, 209". Report delivered by The Gazette (Montreal). http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.234911.506682717.html (accessed January 13, 2009)

Terrorists' Process to Utilize the Internet

History has shown that Islamic extremists are very efficient with the process of establishing new web sites and managing their propaganda on the Internet. Both U.S. government security officials and private Internet security firms would concur with this. Gabriel Wiemann, who is an expert on terrorist use of the Internet attests to this when he cites that the virtues of the Web such as ease of access, lack of regulation, vast potential audiences, and fast flow of information have been turned to the advantage for groups committed to terrorizing societies.[28] Two of these groups include Middle East terror organizations Hezbollah and Hamas. The former group manifested itself on the Internet during their conflict with Israel in 2006, while the latter manipulated the web during this year's conflict with Israel. In the summer of 2006, Hezbollah, by means of their hackers hijacked unsuspecting Web sites where they ran recruitment videos and posted bank account numbers enabling supporters to donate funds to support their cause against Israel.[29] In 2006, the Shi'a Islamic political and paramilitary organization of Hezbollah, based in Lebanon used this powerful tool to tilt international perceptions and opinions in their favor.[30] Three years later, the casual web surfer witnessed Israel's mastery of the Internet's social networking which influenced global opinion in their favor during their

[28] United States Institute of Peace, Special Report of How Modern Terrorism Uses the Internet by Gabriel Weimann (March 2004), Open-file report, USIP (Wash DC March 2006).

[29] MAJ David A. Acosta, "Hezbollah: Deception in the 2006 Summer War", *IO Sphere*, Winter 2008, 19-23.

[30] Acosta, "Hezbollah: Deception in the 2006 Summer War", *IO Sphere*, 20

conflict with Hamas. This they learned from the 2006 conflict.[31] As of this writing, Israel has been seeking free user space donations on the Twitter and YouTube Web sites to keep the international community informed of the war's progress in real-time from their perspective. Countering this effort, Hamas updated its own Web site and hacked into its opponents.[32] At the same time, a oung Israeli Arab was arrested in Jerusalem attempting to recruit a friend for a suicide mission in the Holy Land. The perpetrator was carrying AQ bomb making instructions downloaded from the Internet.[33]

Extremists' Social Networking Service Possibilities.

A social network service is the perfect opportunity for terrorists to remain anonymous with their activity while online because of the communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. The two most popular social networking Web sites here in the US are MySpace and Facebook which are both free. Both sites are very popular here in America because they are interactive with a user-submitted network of friends; contain personal profiles, blogs, groups, photos, music, and videos for teenagers and adults internationally. Currently, Fox News is reporting that extremists are recruiting Somalian Americans via the Facebook

[31] The New York Times Sunday Late Edition. "The Toughest Q's Answered in the Briefest Tweets"; January 04, 2009. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.852026074972280.html (accessed January 05, 2009)

[32] The VNUNET.COM. "Gaza Conflict Mirrored Online"; January 03, 2009. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.646386.3489934341.html (accessed January 05, 2009)

[33] Shoresh, "*International Fellowship of Christians and Jews*", October 2008 Vol 14, No. 10, 3.

network.[34] There are other social networking sites offered but they do not offer the same services. These are Nexopia (mostly in Canada); Bebo, Hi5, Tagged, Xing, and Skyrock in parts of Europe; Orkut and Hi5 in South America and Central America; and Friendster, Orkut, Xiaonei and Cyworld in Asia and the Pacific Islands. Anyone of these networks would allow exploitation if they are not already being manipulated.[35]

Is it a Centralized/Decentralized Approach?

Data gathered for this paper leans towards the terrorists using the Internet to spread their ideological movement in a decentralized manner because of its anonymous nature and the way they conduct their combat operations. Better defined as specialized individual networks, they become terrorist cells and this is changing the way the Islamic extremists operate even to the point where “Al-Qaeda is encouraging its supporters to stay home and train on-line”[36] instead of traveling afar to learn a certain skill. President Bush reinforced this notion when he mentioned that “terrorists spring up in local cells, inspired by Islamic radicalism that is not centrally directed.”[37]

The Jane’s Intelligence Review dated January 01, 2006 offers the best systemic description of the jihadist on-line activity, proving that it operates using a decentralized approach. It describes how the extremist Web sites have a very

[34] Fox News special report, March 17, 2009
[35] Wikipedia, Social Networking, http://en.wikipedia.org/wiki/Social_networking, (accessed December 10, 2008)
[36] NBC News Transcript, “Potential Terrorists Waging Jihad via the Internet”, Aug 22, 2007, http://www.jihadwatch.org/archives/2007_11.php, (accessed Oct 10, 2008)
[37] America.gov- Dept of State. “President Bush Calls for Firm Resolve Against Terrorism, 6 October 2005” http://www.america.gov/st/washfile-english/2005/October/20051006113103adynned0.565.html (accessed October 7, 2008)

brief lifespan because their Internet Protocol (IP) address repeatedly changes.[38] This may be confusing for the average person who is non-literate about computer networks because it would seem that the Web sites need to maintain a "fixed" status in order to remain coherent and relevant concerning the plethora of information that is posted by the terrorists. In reality it is just the opposite. The key to understanding the decentralized online movement is to solve how a single Web site fits into the overall dynamic and interactive network while remaining anonymous.[39]

The same periodical also explains how jihadist Web sites can be categorized into three different classes and how they interrelate with one another. The first are the key nodes known as mother sites, which contain the terrorists' official Web sites and a range of different web forums permitting on-line operations. The second one is classified as the "distributors," which are a host of various Web sites that copy and upload new jihadists' material onto multiple sites, which direct visitors and newcomers to the uppermost Web sites. The third and final group are the "producers," which are a variety of self-styled jihadist' media companies that reproduce the raw material in sleeker and more accessible forms.[40]

Further study illustrates the three distinct types of web sites in detail. Separating the first class, when considering the key nodes, it refers to them as the

[38] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, pg 4- January 01, 2006, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed November 19, 2008).
[39] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, 6.
[40] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, 7.

official homepages of jihadist groups, jihadist clerics, and ideologues on the Internet. But the “mother site” aspect of it comes from the authoritative sources of first-hand information, especially on theological concerns, ideological disputes, strategic thinking, to include doctrines and communication for its webpage visitors.[41] The unofficial Al-Qaeda www.alneda.com Web site referred to earlier, which was shut down in late 2005 is a prime example of a mother site. Another example is the homepage of the famous jihadist intellectual Mustafa Setmariam Naser, otherwise known as Abu Musab al-Suri. In the fall of 2005, it was reported that his Web site was uploaded in a parasitic fashion to a US real estate company without their knowledge.[42] Evidence reflected that this Web site contained the entire library of Al-Suri’s call for an Islamic global resistance since the late 1980’s. Some Islamic scholars will argue that his library is the most important jihadist strategic study ever written.

Current active terrorist groups such as the Al-Qaeda Organization in the Islamic Maghreb (AQIM), which was formerly known as the Algerian Group Salafist for Preaching and Combat (GSPC) maintain a Web site that is also considered a key node. The GSPC declared its faithfulness to AQ in the fall of 2003 and has been involved in several terrorist plots in Europe over the past few years, with the intent to overthrow the Algerian government and institute an

[41] Jane’s Terrorism and Insurgency Center 2005, Information Campaigns, pg 3- March 18,2004, http://www8.janes.com/JDIC/JTIC/document View.do?docID=/content1/janesdata/magsjtic.html, (accessed 23 December, 2008)

[42] Jane’s Terrorism and Insurgency Center 2005, Information Campaigns, pg 5

Islamic state.[43] Another example is the Ansar al-Sunna Army Web site which is illustrated in the next chapter. This organization has been the most prolific in beheading its hostages in Iraq since Abu Musab al-Zarqawi's network introduced this terror tactic. Since his death by coalition forces in June of 2006, new videos of beheadings on the Internet have decreased, but other AQ networks are known to continue this heinous act. This Web site contains the most recent communiqués, ideological tracts, religious fatwas, issues of its on-line journal, their magazine, but most importantly video footage of their operations, and encrypted software.[44] Successful video footage is key to inspiring their followers to hasten their cause and the software is used in order to remain anonymous on the net. Currently, the Ansar al Sunna Army site is unstable and it disappears sometimes and reappears at a new address. In general, this appears to be a problem for many of the official jihadist Web sites. One can only surmise that the reason for this would be to keep those who are 'collecting' on the Web site off-balance.

The linkage from the key nodes to the very flexible Web site distributors is conducted in a decentralized manner. For example, the Ansar al Sunna Army Web site has a mailing list which allows web-surfers to access it right after it reappears at a new address, download its entire content and upload it on numerous

[43] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, pg 8- January 01, 2006, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed November 19, 2008)

[44] Jane's Terrorism and Insurgency Center 2005, Information Campaigns, pg 3- March 18,2004, http://www8.janes.com/JDIC/JTIC/document View.do?docID=/content1/janesdata/magsjtic.html, (accessed 23 December, 2008)

other sites. The jihadist Web site discussions are both key nodes and distributors in the extremist online infrastructure. A handful of sites seem to be serving as the originating source for jihadist textual or audio-visual primary material. However, in general they act as distributors, circulating the material retrieved from elsewhere.[45]

The role of the distributor is performed by different web sites. Even though they are not the primary source for authoritative information and material about the jihadist movement, they are the most significant agent for sustaining the online infrastructure. Their importance is derived from being able to disburse as widely as possible the material received from the key nodes. The distributors can be subdivided into three different categories: First, there are the directories of updated links to external sites. Second, there are the mailing lists and message boards, such as Yahoo! Groups. Then third, there are the non-interactive homepages of sympathizers, which at times happen to be memorial sites.[46]

The directories offer the Web site newcomers a quick overview of the most important sites. As of early 2009, an example of this is the “Jihad, War, Terrorism, and Peace in Islam” Web site, where the browser will find a combination of both pertinent Web sites and the most relevant extremists' blogs.[47]

The entry points into the world of jihadist Web sites are numerous. Often it is

[45] Jane’s Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, pg 6- January 01, 2006, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed November 19, 2008)

[46] Jane’s Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, 8.

sufficient to locate only one jihadist Web site, since many of them feature a list of recommended links, although they may not be up to date. As of this writing for instance, if one were to visit the "Jihad Online: Islamic Terrorists and the Internet" web site, they would be offered many different sub-category options concerning extremism, jihadism, hate crimes, and hyper-links for greater knowledge on the extremist movement.[48]

The mailing lists and message boards are important distributors as well, because they provide easy access to jihadist online resources. Jihadist Yahoo Groups are a good example of an interactive message board and they offer a large supply of free storage space. Yahoo Groups has become one of AQ's most significant ideological bases of operation in supporting their spread of cyber-jihad.[49] To illustrate, the Middle East Media Research Institute Web site[50] offers the visitor a multitude of web postings. Yet another Yahoo Group message board, dated January 17, 2009 is titled "Pak Jihadi groups recruiting young children for Jihad, suicide attacks: Muttahida Qaumi Movement (MQM)."[51] This message board was apparently created for the MQM Party and claimed that banned religious organizations in Pakistan were busy recruiting minors for Jihad and

[47] Jihad, War, Terrorism, and Peace in Islam.Org http://www.uga.edu/islam/jihad.html (accessed January 06, 2009)

[48] Jihad Online: Islamic Terrorists and the Internet Org http://www.adl.org/internet/jihad.asp (accessed January 06, 2009)

[49] Rita Katz & Josh Devon at www.jihad.com, E-Groups abused by jihadists, http://www.adl.org/internet/jihad.asp (accessed January 06, 2009)

[50] The Enemy Within: Where Are the Islamist/Jihadist Web sites Hosted- MEMRI, and What Can Be Done About It? Org http://memri.org/bin/latestnews.cgi?ID=IA37407#_edn6 (accessed January 06, 2009)

[51] Pak Jihadi groups recruiting young children for Jihad, suicide attacks: MQM. Org http://in.news.yahoo.com/139/20090117/874/twl-pak-jihadi-groups-recruiting-young-c.html (accessed January 17, 2009)

using them as suicide attackers. Other sites have online training manuals and handbooks in AQ's Encyclopedia of jihad. For a period of time these web pages did not function in that capacity, rather they were serving as jihad centers for news, documents and communiqués.[52]

Non-interactive Web sites which are maintained by jihadist sympathizers assist in the distributor's success as well. They are sometimes redesigned into sleeker and more user-friendly formats where jihadist materials are posted. The memorial Web sites are occasionally dedicated to jihadist commanders. One noted commander is Emir Khattab, who is the model of the Arab mujahideen movement in the Cauacasus. They also post recent communiqués and Osama bin Laden's speeches in various document formats, including brief summaries of his main points. Also offered are the collected works of key Saudi jihadist ideologues such as the deceased Yusaf al-AYiri, Sultan Utaybi, and Faris bin Ahmad. As opposed to quite a few other distributors, the Al-Qa'idun Web site at: http://www.free-minds.org/taxonomy/term/8 is conceited because it claims that it is responsible for the multiplication of all jihadist materials in digital form.[53] This simply can not be true because of the terrorists' decentralized nature of dissemination operations.

The third category supporting the jihadist Web sites is the producers. Their function is to reformat the jihadist raw material into a neater and more

[52] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, pg 11- January 01, 2006, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed November 19, 2008)

[53] Discover True Islam at Free Minds. Org http://www.free-minds.org/taxonomy/term/8 (accessed December 7, 2008)

attractive manner before it is distributed on the web.[54] As of 2006, the most active producers were the Global Islamic Media Front (GIMF) which consists of the Electronic Media Battalion and the Islamic Media Center, whose main base operates out of Canada. They send out e-mails to other media outlets as needed concerning any matters that are anti-Islam.[55] Extremists sustain this program through a 24/7 global jihad.[56] GIMF was once an important group to the online jihad support community, many of whom did not speak Arabic. The GIMF is known as one of the oldest and far reaching propaganda media-distribution enterprise networks with its beginnings as early as 2002.[57] The group's main contribution was in translating Arabic statements into German, French, and English for wider dissemination.[58] What is most important is that the GIMF has issued a directive for the online Islamist extremist community to infiltrate Muslim and non-Muslim Web sites and post propaganda in support of Al Qaeda. The site instructs sympathizers on how to repel the intensive Western media campaign

[54] Jane's Intelligence Review, Al-Qaeda Online- Understanding Jihadist Internet Infrastructure, pg 9- January 01, 2006, http://www.janes.com/articles/Janes-Intelligence-Review-2006/Al-Qaeda-online-understanding-jihadist-internet-infrastructure.html, (accessed December 10, 2008)

[55] Agence France Press – English. "Austrian Politician Threatened After Anti-Islam Comments: Ministry, January 15, 2008". Vienna. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.744796507875964.html (accessed December 1, 2008)

[56] National Post (f/k/a The Financial Post) (Canada). "Did Snowball Video Hide Terror Plot; Al QaedaLinks, February 12, 2008". National Post, Toronto, Canada. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.852026074972280.html (accessed December 1, 2008)

[57] The Globe and the Mail (Canada). "A Media-Distribution Enterprise for Global Terror, May 22, 2008". International News; Global Islamic Front. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

[58] The Jawa Report. "Two More German GIMF Online Jihadis Arrested, November 25, 2008". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.413091782222758.html (accessed December 1, 2008)

directed at Al Qaeda and on what must be accomplished in order to be effective.[59] They gather, reshape, and distribute jihadist material and they also serve as recruitment centers for would-be electronic jihadists. Their propaganda comes in many forms such as video clips of roadside bombs blowing up coalition forces, and tracts describing the world's most influential Islamist insurgencies. There is even a video game known as the "The Night of Capturing Bush," where the players try to kill our forty third president and the game climax is one-on-one combat against him.[60]

Late 2007, the GIMF was recruiting English translators on its web site to keep pace with the daily output of terror news.[61] During that same timeframe, even Youtube carried several of the GIMF propaganda videos. These were unknowingly hosted by Snapy Communications Incorporated, located in Coral Springs, Florida via FreehostiaFreehostia.com.[62] There are other US Web sites that host extremist web pages without their knowledge. Another example is where the GIMF has been linked with two Americans, Abu Mansour and Daniel Joseph Maldonado aka Daniel Aljughai. They were involved in the AQ's struggle in Somalia that is affiliated with the Movement of Jihadi Youth which is linked to

[59] The Jawa Report. "Wordpress Hosted Terrorists Announce Media Campaign to 'Infiltrate' Infidel Web sites, Support Al Qaeda, pg 1-2, July 13, 2007". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.362011693525109.html (accessed December 1, 2008)

[60] The Jawa Report. "Wordpress Hosted Terrorists Announce Media Campaign to 'Infiltrate', 4.

[61] BBC Monitoring Europe – Political Supplied by BBC Worldwide Monitoring. "Islamist Arrested in Austria Was Head of German GIMF – Web site, September 13, 2007". Excerpt from report by German Spiegel Online web site on September 12, 2007. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

[62] The Jawa Report. "Attn. Jawas and Youtube Crusaders: GIMF Web site, December 5, 2007". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-0.164738.620333730.html (accessed December 1, 2008)

an AQ organization.[63] Going one step further, Samir Khan who is a North Carolina resident released a propaganda video through the GIMF titled "Caravan of Martyrs in Iraq."

The message of this video is "Kill the Cross Worshippers (Christians)." It has taken various clips from martyrdom videos and spliced them together but maintained their water marks from Zarqawi's old Mujahideen Shura Council, Ansar al-Sunna, and the Islamic State of Iraq.[64] Not only is the GIMF specializing in extremist propaganda but it has been known to raise funds from contributors to the jihad. This GIMF charity case in particular is German based and focused on collections for the Taliban with an on-line promise that 100% of all donations will arrive in Afghanistan.[65] A good news story here is that the GIMF is also being monitored by specialized agencies worldwide. For instance, three men were arrested in Europe late August 2007 for their plot to attack U.S. interests in Germany. They confessed that they were influenced by the GIMF AQ propaganda video tape media.[66] Taking all of this GIMF data into consideration, it appears that the organization is a virtual union of global sympathizers for

[63] The Jawa Report. "The American Leader of Al Qaedain Somalia and its U.S. Web site, February 8, 2008". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-0.552017.667519749.html (accessed December 1, 2008)

[64] The Jawa Report. "New GIMF Video: Caravan of Martyrs in Iraq, November 6, 2007". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-0.552017.667519749.html (accessed December 1, 2008)

[65] BBC Monitoring Europe – Political Supplied by BBC Worldwide Monitoring. "German Paper Says Islamist Collecting Internet Donations, April 15, 2008". Report by Yassin Musharbash: "German- Language Islamists Collect for the Taliban on the Web". http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

[66] The Jawa Report. "Three GIMF Online Jihadis Arrested in Austria, September 12, 2007". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-0.79854.5248522815.html (accessed December 1, 2008)

Islamic extremism. The GIMF Web sites are reinforcing “urgent pleas for the Mujahidin needing every assistance now” in their chat rooms, where specific instructions are provided on how to give supporting their cause.[67] If a supporter is not able to give financially there are other ways to assist:

> If, however, you do not possess the expertise… there are other matters you can (promote): for example, posting matters related to the raid in most (jihad) forums… posting (material) in non-jihad forums, posting in non-Islamic such as music forums, youth forums, sports forums, and others. Anyone who undertakes to post the material must look into the (appropriate) manner of spreading (the material for each type of forum). The way in which members of music forums address one another differs from the way members of jihad forum address one another.[68]

One can find their symbols and colorful images depicted in Figure 1 on many extremists’ Web sites and their publications are valuable sources of information about the jihadist movement. In October 2004 for example, the GIMF distributed a 500-page electronic book they had fabricated about the terrorist group Tawhid wa’l-Jihad in Iraq, which at that time had limited information about it in the public domain.[69] There have been occasions noted where the producers act as key nodes or mother sites and distributors, replicating the other two categories of jihadists’ Web sites. There are two examples of this.

[67] BBC Monitoring Europe – Political Supplied by BBC Worldwide Monitoring. “German Paper Says Islamist Collecting Internet Donations, April 15, 2008”. Report by Yassin Musharbash: “German- Language Islamists Collect for the Taliban on the Web”. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

[68] The Jawa Report. “Wordpress Hosted Terrorists Announce Media Campaign to ‘Infiltrate’ Infidel Web sites, Support Al Qaeda, July 13, 2007”. Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.362011693525109.html (accessed December 1, 2008)

[69] The Jawa Report. “Wordpress Hosted Terrorists Announce Media Campaign to ‘Infiltrate’ Infidel Web sites, Support Al Qaeda, June 13, 2007”. Report delivered by Newstex. http://mypetjawa.mu.nu/archives/188282.php (accessed December 15, 2008)

The Sahab media, often named AQ's media company and the GIMF's Voice of the Caliphate Broadcast launched in late- 2005.

Figure 1.

The Global Islamic Media Front LOGO Banner[70]

The Sahab media company often produced and packaged Al-Qaeda's senior leadership special messages whereas the GIMF broadcast had started weekly 20 minute news broadcasts which replicated a jihadist version of 'Internet TV'. As of the Jane's writing, Sahab only released four versions of the communication, but the periodical claims that others had attempted to do the same with some failing to achieve success. Nonetheless, the GIMF's Voice of the Caliphate Broadcast was considered a success with the jihadists because it was advertised well in advance and gained great notoriety in Western media coverage.[71] When articles like the news broadcasts were posted on the web via the mother node, the distributors would upload the item in various formats and to multiple links. The second edition of the Voice of the Caliphate Broadcast media file was tracked to 13 different links for downloading. Subsequently, the distributor also called upon visitors to help them dispense the file through a GIMF

[70] The Jawa Report, "GIMF Logo", http://mypetjawa.mu.nu/archives/cat_gimf.php, (accessed December 16, 2008)

[71] Spiegel Online International. "*Al-Qaida's German Blog*", pg 2 http://www.spiegel.de/international/0,1518,434404,00.html (accessed December 15, 2008)

Web site designed especially to disseminate it via free web-hosting sites, where large video files were able to be uploaded free of charge.[72]

The jihadist infrastructure on the Internet is a very flexible and extremely interactive strategy with a high degree of redundancy,[73] as illustrated, and it has advanced considerably within the past seven years. Its abundant and diverse sites constantly nourish and support each other, which makes them difficult, but not impossible to pursue. Its complexity yearns for leadership and oversight.

Adam Yahiye Gadahn who is an American-born, English-speaking senior operative and is currently believed to be the GIMF managing media advisor. Not only does he advise the GIMF but he personally appears in videos for AQ against the US with conviction and has been doing so for the past three years.[74] The number two AQ senior member, Ayman al-Zawahiri has even recognized him as the group's media spokesman directed at the West. AQ considers him a valuable asset for their media efforts because he acts as a "translator, video producer, and cultural interpreter."[75] He is wanted for treason against this country and there is a 1 million dollar reward for his capture.[76] Even if Mr. Gadahn gets captured, it will not slow the GIMF's production capability because of how the organization is structured.

[72] Spiegel Online International. "*Al-Qaida's German Blog*", 4.

[73] Internet source, 01 Jan 2006, Jane's Intelligence Review, AQ Online: Understanding Jihadist Internet Infrastructure

[74] Wikipedia, Adam Yahiye Gadahn , http://en.wikipedia.org/wiki/Adam_Gadahn (accessed October 28, 2008)

[75] The New Yorker. "Azzam the American; The Making of an AQ Homeowner"; January 22, 2007. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.542359.850258951.html (accessed December 01, 2008)

[76] Department of Justice Press Conference, Subject: Federal Indictment of American Terror Suspect Adam Gadahn, (October 11, 2006), Open-file report, Dept of Justice (Wash DC 2006).

III. Case Study – Illustrating the Terrorists in Action on the Net

Terrorists and Their Finance Operations Via the Internet

Like many other political organizations, terrorist groups use the Internet to raise funds. Al Qaeda, for instance, has always depended heavily on donations, and its global fund-raising network is built upon a foundation of charities, nongovernmental organizations, and other financial institutions that use Web sites and Internet-based chat rooms and forums. Even prior to September 11, 2001, evidence reflects that particular terrorist groups were exploiting the Internet for their fundraising. Research indicates that as early as July 1999, our government imposed the first set of sanctions on Afghanistan's Taliban movement for collecting legal tender here in this country in order to accommodate and safeguard Bin Laden.[1] Then in May 2001, just four months prior to the 9/11 attacks the fundraising denial objective was reaffirmed during the Senate testimony of Richard Newcomb, then director of the US Treasury Department's Office of Foreign Assets Control. During his testimony, Newcomb described how his agency's Foreign Terrorist Asset Tracking Center works with other US government agencies to counter the terrorist threat. He cited the center's responsibilities as denying terrorist groups' access to the international financial system, impairing their fund-raising abilities, and blocking their financial

[1] Jane's Terrorism and Insurgency Center 2005, Information Campaigns, pg 3- March 18,2004, http://www8.janes.com/JDIC/JTIC/document View.do?docID=/content1/janesdata/magsjtic.html, (accessed 23 December, 2008)

transactions.[2] Obviously, this center has failed in its prevention attempts, although it has probably mitigated their progress. Still, multiple reports reflect that despite attempts to restrict terrorists' access to funds, their ability to do so remains unhampered on the Internet.

Terrorist groups continue to use Web sites and chat rooms to appeal directly to their supporters for funding, making it increasingly difficult for law enforcement agencies to disrupt their illegal activities. According to Todd Hinnen, a terrorist financing expert who served on the Bush administration's National Security Council, the jihdists use the Internet in two different ways to solicit and collect funding and equipment in support of terrorist operations.[3] The most popular way appears to be through multiple means of solicited donations, indoctrinated adherents, shared information, and recruited supporters directly via Web site chat groups, and targeted electronic mailings. The second way benefiting the extremists is to take advantage of charitable organizations on-line, soliciting funds with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors' largesse to fund acts of violence. The third way is for the terrorists to perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support their mission with the proceeds of such crimes.[4]

[2] Jane's Terrorism and Security Monitor, *US Proscriptions, No Cure for Islamic Internet Fundraising*, 01 Jun 2001, http://jtsm.janes.com/public/jtsm/index.shtml, (accessed December 06, 2008)

[3] Benjamin R. Davis, The Catholic University of America CommLaw Conspectus, *"Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet"* (Fall 2006):14.

[4] Davis, The Catholic University of America CommLaw Conspectus, *"Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet"* (Fall 2006):15.

For example the United Kingdom (UK) -based, Hamas front-organization--Interpal--is one of the largest Internet-based fundraising organizations and utilizes several of those techniques already mentioned In addition to being a principal conduit through which funds are funneled under the guise of a Hamas charity, "Interpal is a fundraising and coordination point for other Hamas-affiliated charities. As such, Interpal supervises activities of, and develops new charities in targeted areas, instructs how funds should be transferred from one charity to another, and even determines public relations policy."[5] Despite enforcement actions by the United States and Israel to freeze the assets of Interpal and shut down the Web site, the organization continues to operate and raise funds online.

Some prominent Islamic extremists issue public statements and writings referring followers to Web sites that provide instructions on how to exploit the Internet and raise funds for their deadly campaigns. Imam Samudra, an Indonesian AQ terrorist and leader of the 2002 Al Qaeda Bali bombings, recently released an autobiography from his jail cell containing a chapter entitled, "Hacking, Why Not?"[6] The chapter details basic information on money laundering, online credit card fraud, and computer programming languages, exhorting all would-be terrorists to use cyberspace to further jihad.[7]

[5] Davis, The Catholic University of America CommLaw Conspectus, *"Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet"*, 21.
[6] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace", *Alleged Terror Hackers Arrested* (July 2005):2.
[7] Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace", *Alleged Terror Hackers Arrested*, 4.

The Hezbollah terrorist network has combined multiple communications media to raise funds for terrorism-related operations. For example, the group maintains its own popular television station, Al Manar, which is broadcast throughout the Middle East, and promotes violence against Israel and the United States. Al-Manar's Web site urges contributions "for the sustenance of the Intifadah" [8] and provides bank accounts in Lebanon to which donations can be made for the purpose of carrying out violence against Israeli interests. The Sunni extremist group, Hizb al-Tahrir, uses an integrated network of Internet sites, stretching from Europe to Africa, which asks supporters to assist by giving money and encouraging others to donate to the cause of jihad. Banking information, including the numbers of accounts into which donations can be deposited, is provided on a site based in Germany.[9] Another terrorist group identified as the fighters in the Russian breakaway republic of Chechnya have likewise used the Internet to publicize the numbers of bank accounts to which sympathizers can contribute.

Each of these Internet fundraising techniques illustrates terrorists' strategic manipulation and sophisticated use of readily-available technology in order to raise funds for militant campaigns. Terrorist Web sites, chat rooms, and other forums make use of the Internet for fundraising. These Web sites often use the argument that every Muslim has a duty to advocate the jihad, but that direct

[8] Al Manar Television, http://www.manartv.comlb/NewsSite/News.aspx?language, pg 2, (accessed November 15, 2008)

[9] Al Manar Television, 4.

participation in operations is not required of everyone. The appeal itself for one's financial support is a method of permitting an individual to feel that they have fulfilled their duty as a Muslim, while not needing to change their lifestyle and join the actual fight.[10]

The Internet exacerbates the jihadist fund raising problem for the authorities in two respects. One is that since a charity can locate itself anywhere in the world, even in a state that sponsors terrorism or a country that does not regulate charitable organizations through the Internet, it can obtain access to donors worldwide. Secondly, a charity that exists on the Internet is not generally kept under surveillance to verify its legitimacy nor is it subject to regulators as are other tangible charities.[11] A case study for this is the UK effort to prevent terrorists from sending money through their charities. The UK Government has established a counter-terrorism agency to respond to their fundraising. Its program is based on a prevent- pursue- protect- and prepare strategy and a concept of making arrests, seizing cash, freezing assets, and upsetting terrorist planning activity when provided the opportunity. The program's Detective Superintendent, Mark Holmes, has remarked that some potentially dangerous individuals have been taken out of action as a result of this effort.[12] One particular example is the foiled plot of a courier, whose cash was seized at

[10] Deputy Assistant Secretary of Defense Support to Public Diplomacy, Before the Committee on Homeland Security and Governmental Affairs by Statement of Michael S. Doran (May 3, 2007), Open-file report, US Senate (Wash DC 2007).

[11] The Investigative Project on Terrorism, pg 2, December 03, 2008: Articles by IPT http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e6172662e70.html (accessed December 17, 2008)

[12] The Investigative Project on Terrorism, 4.

Heathrow Airport. His intent was to assassinate King Abdullah, the leader of Saudi Arabia in 2007.[13]

Another fundraising technique is where Internet user demographics (culled, for instance, from personal information entered in on-line questionnaires and order forms) allow terrorists to identify users with sympathy for a particular cause or issue. These individuals are then asked to make donations, typically through e-mails sent by a front group (i.e., an organization broadly supportive of the terrorists' aims but operating publicly and legally, usually having no direct ties to the terrorist organization).[14] For instance, money benefiting Hamas has been collected via the Web site of a Texas-based charity, the Holy Land Foundation for Relief and Development (HLF). The U.S. government seized the assets of HLF in December 2001 because of its ties to Hamas. The U.S. government has also frozen the assets of three other seemingly legitimate charities that use the Internet to raise money. These sites are the Benevolence International Foundation, the Global Relief Foundation, and the Al-Haramain Foundation because of evidence that those charities have funneled money to Al Qaeda.[15]

To cite another example, in January 2004, a federal grand jury in Idaho charged a Saudi graduate student with conspiring to help terrorists' organizations.

[13] Jane's Terrorism and Insurgency Center, Jane's Police Review Community, March 7, 2008: Counter-Terrorism Conference – Terrorists take UK Charity Cash to Fund Extremist Networks http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e6172662e70.html, (accessed August 30, 2008)

[14] 9/11 Commission Report, "*National Commission on Terrorist Attacks Directed Against the US*", pg 5, (May 2006), Open-file report, USIP (Wash DC March 2006).

[15] 9/11 Commission Report, "*National Commission on Terrorist Attacks Directed Against the US*", 7.

These organizations were waging jihad by using the Internet to raise funds, field recruits, and locate prospective U.S. targets located in the Middle East. Sami Omar Hussayen the suspect was also a doctoral candidate in a computer science program at the University of Idaho who at time was ironically sponsored by the National Security Agency. He was accused of creating Web sites and an e-mail group that disseminated messages, then coordinating with two radical clerics in Saudi Arabia who supported jihad.[16] Web site possibilities are numerous not only for financial donations but also for jihad supporters and the next subsection will illustrate several of these.

Web sites that Benefit Exploitation for the Extremists

Al-Jazeera is one of the most popular Islamic terrorist' Web sites because the word means "The Island or Pennisula," referring to their status as the only independent Middle Eastern news station. Not only can the terrorists get their message out through them but they can also monitor how well it is being received through the number of hits on the portal.[17] Its television headquarters is located in Doha, Qatar and has expanded into a network with several outlets, focusing on the Internet in multiple languauges, and in several regions of the world. On July 4, 2005, Al Jazeera officially announced plans to launch a new English-language satellite service to be called Al Jazeera International.[18] The new channel with the Internet site started on 15 November 2006 under the name Al Jazeera English and

[16] United States Institute of Peace, Special Report of How Modern Terrorism Uses the Internet by Gabriel Weimann (March 2004), Open-file report, USIP (Wash DC March 2006).

[17] Wikipedia, Al-Jazeera, http://en.wikipedia.org/wiki/Al_Jazeera , pg 4, (accessed 28 October 2008)

[18] Wikipedia, Al-Jazeera, 6.

has broadcast centers in Doha (next to the original Al Jazeera headquarters and broadcast center), London, Kuala Lumpur and Washington D.C. The station's research shows "some of the world's one billion English speakers, including Americans, thirst for news from a non-Western perspective."[19]

The Al Jazeera Web site can be visited at any time to see how it is reporting news items concerning the West. An interesting point here is that the station first gained widespread attention in the West following the September 11, 2001 attacks, when it broadcast videos in which Osama bin Laden and Sulaiman Abu Ghaith defended and justified them. This led to significant controversy and accusations by the United States government that Al Jazeera was engaging in propaganda on behalf of terrorists. Al Jazeera countered that it was merely making information available without comment and, indeed several western television channels later followed suit in broadcasting portions of the tapes.[20]

Figure 2 depicts the Islamic Army in Iraq (IAI), another popular Web site that the terrorists favor. The group has always been keenly aware of the value of successful information operations and has been a prolific producer of high-quality videos and communiqués distributed via the Internet. The IAI has fused propaganda with action in the kidnapping and exploitation of foreign hostages,

[19] CNN World.com, Al-Jazeera Turns its Signal West, 4 July 2005, OSINT, http://web.archive.org/web/20050710010536/http://www.cnn.com2005/world/meast (accessed 28 October 2008).

[20] Answers.com, Al-Jazeera, OSINT,http://www.answers.com/topic/al-jazeera (accessed 28 October 2008).

then posting the videotapes on the Web.[21] At an initial glance of the Web site, one will see that the IAI seems to have a moderate Islamic ideology and its own political program which stresses its own political goals separating itself from Western democratic principles.[22] But even as Coalition Forces are reduced in Iraq in the future, this Web site will continue to influence those who observe it. According to Dr. Ali al-Naimi, Media Spokesman for the IAI, "their top goals are eliminating occupation of any kind and putting an end to its effects so that they can establish their fair, equity and rights of all Iraqi society and sects in one state."[23]

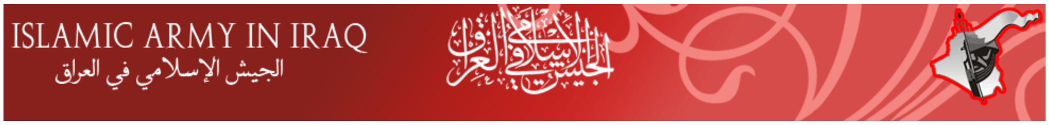


Figure 2.

The Islamic Army of Iraq LOGO Banner[24]

Further study reveals that there is much more to this portal. The site reveals numerous anticoalition stories, photos, and logos. Stories and photos

[21] Islamic Army In Iraq, OSINT, http://iaisite-eng.org/index.php?option=com_content&task=blogcategory&id=22&Itemid=45 (accessed October 28, 2008).

[22] Jane's Terrorism and Insurgency Center, Jane's Police Review Community, June 23, 2008: Information Campaigns of Extremist Networks http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)

[23] Islamic Army Iraq, OSINT, http://iaisite-eng.org/index.php?option=com_content&task=blogcategory&id=22&Itemid=45 (accessed October 28, 2008).

[24] IAI Logo, http://iaisite-eng.org/index.php?option=com_content&task=blogcategory&id=22&Itemid=45, (accessed December 10, 2008

focus on the terrorists' tactical successes from vehicle ambushes, Improved Explosive Device (IED) attacks, indirect fire strikes, suicide bombings, and battle damage assessment on US Forces.

A third Web site, founded in May 2007 that terrorists exploit is the Al-Furqan Institute for Media Production known as "The Long War Journal." Its origin is in New Jersey and is supported by the Public Multimedia Inc. which is a nonprofit organization. This site, located at http://www.longwarjournal.org/archives/2007/10/us_targets_al_qaedas.php, hosts stories, issues, featured reports from a global standpoint, and an archive of photos concerning AQ. This is also a network of video production cells which supports the manufacture and distribution of videos showing Al Qaeda claimed attacks (or those of allied insurgent groups) and celebrating the deaths of martyrs.[25] Figure 3 illustrates a LOGO based on "The Five Hard Years." Of interesting note is that the collage of photos captures President Bush in anguish, the insurgents in action, and the nation's political and military senior leadership in prayer over the war.

[25] Jane's Terrorism and Insurgency Center, Jane's Police Review Community, March 7, 2008: Information Campaigns of Extremist Networks http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)

Figure 3.

An Illustration of “The Hard Five Years”[26]

The fourth Web site to be analyzed belongs to Ansar al-Sunna (AS), formerly known as Ansar al-Islam hyperlinked to http://mypetjawa.mu.nu/ archives/057937.php. Its LOGOs are illustrated in Figure 4 with the familiar black flags that are found on numerous other extremist’s web pages. It is a Sunni extremist group of Iraqi Kurds and Arabs with the intent on establishing a Salafist Islamic state in Iraq under Sharia law, a strict interpretation of Koranic instruction. The group regularly targets Coalition forces, Iraqi Government and security forces, and Iraqi political parties on its site. Ansar al-Sunna has claimed responsibility for many high-profile attacks in Iraq, including the suicide bombing of a US military dining facility in Mosul in December 2004 that killed 22 US and Coalition soldiers. Ansar al-Sunnah continues to conduct and claim responsibility for car bombings, assassinations and kidnappings in Iraq, which the group posts and archives on its site.[27] The group is believed to have members located

[26] The Long War Journal, “The Hard Five Years” collage, http://www.longwarjournal.org/archives/2007/10/us_targets_al_qaedas.php, (accessed November 30, 2008)

[27] National Counter Terrorism Center, 2008 Counter Terrorism- Ansar Al Sunna, http://www.nctc.gov/site/groups/as.html, (accessed October 29, 2008)

throughout Europe and possibly the United States, which is an important point concerning the development of home-grown terrorists.

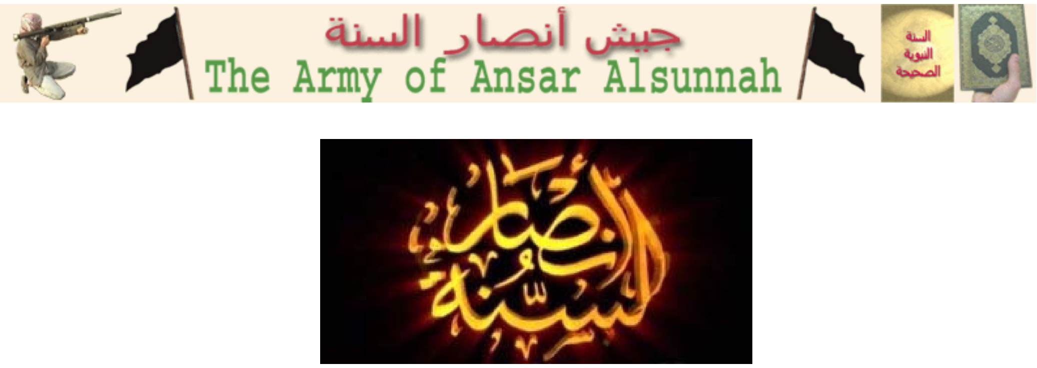


Figure 4.

The Army of Ansar Al Sunnah Logo and Banner[28]

The fifth example is one of the most disturbing and gruesome Web sites. It demonstrates the Juba Sniper's success in shooting our soldiers and can be found on several links. Its primary Internet Provider address is: http://video.google.com/videoplay?docid=-8302187367555388286 and its banner is located in figure 5 below. The streamlined video version on the Web site is over fifteen minutes long and during this timeframe, the shooter engages 29 different soldiers in different locations.[29] This killer(s) is so effective at this that the soldiers around the casualty initially do not know what is going on or how to react to it.

[28] Wikipedia, The New Ansar Al Sunna Logo, http://en.wikipedia.org/wiki/Ansar_al-Sunnah, (accessed December 10, 2008)
[29] "Juba Sniper Full 15 Minutes in Baghdad", pg 1, http://video.google.com/videoplay?docid=-8302187367555388286, (accessed October 1, 2008)

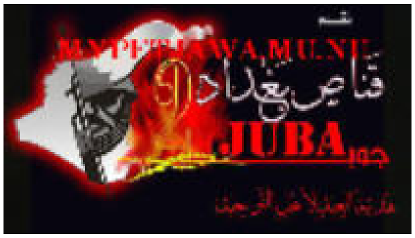


Figure 5.

The Baghdad Juba Sniper Trademark[30]

According to the Web site, the only indication that Juba is the same individual in each time of these incidents is a single bullet casing and a note left behind at the location where he is believed to have been. The message reads in Arabic, "What has been taken in blood cannot be regained except by blood, Baghdad Sniper."[31] These items were found in nearby buildings after the attacks. "Juba's" existence, however, is not proven. He could be one person or a combination of many different insurgents. It is also possible that Coalition forces have killed one or more "Jubas," but each time a new one emerges.[32]

The most recent video shows a black-masked man identified as "Juba, the Baghdad Sniper" and shows him prowling Baghdad in search of unwary American troops. At one point Juba is seen adding another "kill" to a list of 37 on a piece of paper on a wall. Possibly, the film is a collection of videos of different snipers at work. It also contains an interview with someone described as commander of the Baghdad sniper division. The subsequent footage shows

[30] The Juba Sniper Logo, http://video.google.com/videoplay?docid=-8302187367555388286, accessed December 10, 2008)
[31] "Juba Sniper Full 15 Minutes in Baghdad", 3.
[32] Its a New World, January 29, 2006- "*Juba = Baghdad Sniper*", pg 2, http://baghdadtreasure.blogspot.com/2006/01/juba-baghdad-sniper.html, (accessed October 1, 2008)

numerous insurgents being trained in the use of sniper rifles. The video focuses on the fear insurgency snipers create among US soldiers.[33] The terrorists' sniper video remains on the Internet as of early Jan 2009. This grisly video of American soldiers being shot by an unknown gunman appears to be a revised version of the Juba clip.[34]

The films are important for two reasons. Two years ago, combat operations had highly accurate snipers hunting US soldiers. The most effective weapon used by insurgents hitherto has been a bomb in or beside the road - the notorious IED (improvised explosive devices). As of late 2006, these IED's have caused at least 998, or 35 per cent of US combat deaths. In contrast, there are no precise figures from the American side for casualties caused by snipers but 272 soldiers have been killed by small arms fire and a further 425 by unspecified hostile fire for the same time period.[35]

These five illustrated Web sites provide the reader with different examples on how the extremists benefit from Internet exploitation. They represent how the radical communicates their hatred message for recruiting purposes to the success of killing our uniformed soldiers down range. Internet chat rooms are another avenue for communiqué and exploitation which will be discussed in the next subsection.

[33] "*Juba = Baghdad Sniper*", 4.

[34] "*The Training of a Sniper*", December 13, 2008, http://www.archive.org/details/Al-ansarMediaAnsarAl-islam-TheSniper, (accessed January 19, 2009).

[35] The Independent World, "Conflict in Iraq: The Sniper Who Shoots on Video", November 9, 2006, http://baghdadtreasure.blogspot.com/2006/01/juba-baghdad-sniper.html, (accessed October 31, 2008)

Terrorists' Use of Chat Rooms

One of the Internet's primary mediums that terrorists use to influence their audiences is through chat rooms, which are growing in popularity. This is currently evident in Europe because both the British and the Australians are investigating these occurrences, since they have been attacked or seriously threatened. Three examples illustrate this chat room tactic. The first example, reported by the Jane's review occurred in April of 2007 and involved a pro-jihadist Internet forum using a chat room to facilitate a live interview with a purported Palestinian ISI member. This interview centered on the participants asking the facilitator about the progress of the Jihad in Iraq and how they could participate in "martyrdom" operations.[36]

The second example took place in April of 2008 and involved a 23 year old male along with his 23 year old cousin who was possibly plotting to attack members of the British Royal Family. They influenced a 16 year old British boy to assist in carrying out this mission, who was later arrested at Heathrow Airport for having in his possession extremist material and all the necessary ingredients to make homemade bombs downloaded from the Internet.[37] The documents explained and illustrated how to kill non-Muslims, how to make suicide vests, and had personal information and addresses on 15 members of the Royal Family. The hardware for the explosive devices included ball-bearings and remote detonators.

[36] Jane's Intelligence Review, Jihad Online- "*The Changing Role of the Internet*", pg 2, August 01, 2007, http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)
[37] Jane's Intelligence Review, Jihad Online- "*The Changing Role of the Internet, 4.*"

These three met on-line and carried out their plans through designated chat rooms.[38] The British constables who arrested the 16 year old boy pointed out: "his case should serve to highlight the perils of young people flirting with radicalism and violent jihad on the Internet and elsewhere."[39] They reinforce the development of the home-grown terrorists' threat from the Internet, which is the concept that this paper is attempting to prove.

The third example involved a story picked up by two separate Sunday Australian Newspapers late April 2008. The theme of both articles was the Austrailian Government warning parents to "police" their children while using the Internet because extremists were using chat rooms to recruit for the jihad. The Sunday Tasmanian reading noted that while the government was "trawling Islamic web and chat sites, two apparent conversations between Australians and foreign extremists were on-going."[40] The other Sunday edition- "Territorian, highlights that a certain chat room entry had a young Melburnian appearing to be speaking with a radical recruiter based in Pakistan."[41] Even though this problem appears to only be persistent in the United Kingdom (UK) and Australia, one would have to wonder why it is not monitored as much here in America. The

[38] The Press Association Newsfile, "Terror Cyber Grooming Leader Jailed for 12 Years", August 19, 2008, http://www.lexisnexis.com/us/Inacademia/frame.do?tokenkey=rsh-20.717161.56119410.html, (accessed October 16, 2008)

[39] The Press Association Newsfile, "Terror Cyber Grooming Leader Jailed for 12 Years", August 19, 2008, http://www.lexisnexis.com/us/Inacademia/frame.do?tokenkey=rsh-20.717161.56119410.html, (accessed October 16, 2008)

[40] The Sunday Territorian (Australia), "Islamic Extremists Turn To Cyberspace", June 29, 2008, http://www.lexisnexis.com/us/Inacademia/frame.do?tokenkey=rsh-20.500045.14275430.html, (accessed October 16, 2008)

[41] The Sunday Tasmanian (Australia), "Chatroom Terrors Alert Warning On Islamic Extremists", June 29, 2008, http://www.lexisnexis.com/us/Inacademia/frame.do?tokenkey=rsh-20.448698.44321743.html, (accessed October 16, 2008)

argument here is that our freedom of speech which is the freedom to speak freely without censorship or limitation would be violated.

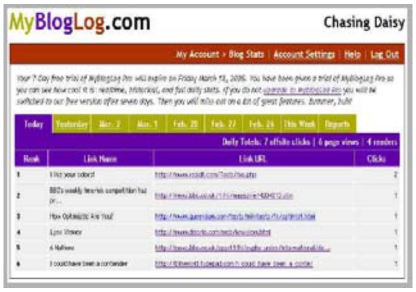
Some select chat rooms can be dangerous for our youth to be surfing, regardless of where they are located. They can be a breeding ground for the terrorists as well. Another way the extremists communicate with their potential followers is through the posting of blogs which will be discussed in the next subsection.

Extremists' Use of Blogs.

Extremists have used blog Web sites just as effective as the chat room. Usually, a site is maintained by an individual with regular entries of extremist propaganda, commentary directed against the West, manipulated photos of civilian casualties, descriptions of successful attacks against our military and other media, such as graphics or video. The author normally displays his personal thought entries in reverse-chronological order and will occasionally post hyper-links to other terrorist web sites reinforcing their ideology. An example of how a terrorist can set up a free Blog, then establish and maintain a dialogue with its sympathisers is pictured in Figure 6. The ease of this is somewhat frightening because there is no oversight or regulation of who the blogger is or the threatening information he may be posting. Yahoo has made beginning a blog so simple that even a computer illiterate terrorist can generate one at either https://www.blogger.com/start or http://www.mybloglog.com/.[42] If a visitor

[42] Starting my own Blog, https://www.blogger.com/start; http://www.mybloglog.com/, (accessed December 10, 2008).

follows the Web site's easy step by step instructions he can generate a posting. Getting started will prompt you to register with your Yahoo ID, add a photo and set up your profile. When you visit MyBlogLog-enabled sites, your photo shows up as a virtual calling card. Clicking on your photo leads to your profile and all the information you share. There is even a way you can add a blog community with similar interests to your profile. Once up and running with your site, you can check your stats, see what people read and where they went next. This is an excellent way for extremists to interact with their followers and solicit ideology.



Your 7 Day free trial of MyBlogLog Pro will expire on Friday March [illegible], 2006. You have been given a trial of MyBlogLog Pro so you can see how cool it is: realtime, historical, and full daily stats. If you do not upgrade to MyBlogLog Pro you will be switched to our free version after seven days. Then you will miss out on a lot of great features. Bummer, huh?

Daily Totals: 7 offsite clicks | 6 page views | 4 readers

Rank	Link Name	Link URL	Clicks
1	I like your colors!	[illegible]	2
2	BBC's weekly fee-ish competition ha pr...	[illegible]	1
3	How Optimistic Are You?	[illegible]	1
4	Lynx Viewer	[illegible]	1
5	6 Nations	[illegible]	1
6	I could have been a contender	[illegible]	1

Figure 6.

Potential Extremist Free Blog Web site Illustration.[43]

The advantage with the blog over the chat room is that it is a vehicle for dialogue between the host and its visitors yet, at the same time, remains a diary. It can be used as a guide for its followers, or used to collect free information about our military. For example, posting sensitive photographs to a blog (especially those showing the results of IED strikes, battle scenes, casualties, and

[43] The Basic Web Page of a Blog Site, http://www.mybloglog.com/, (accessed November 30, 2008)

destroyed or damaged equipment) is providing information which enhances the enemy's targeting process.[44] Of particular interest is the media blog comprised of videos, which is labeled the vlog.[45]

The blog has multiple visual characteristics. It may consist of additional follow-on graphic links and subsequently be labeled a linkblog, or a site containing a portfolio of sketches identifying it as a sketchblog or even one composed of photos, called a photoblog. Another type of blog that extremists may manipulate is the tumbleblog which has a combination of mixed media types. The expanded, collective community of all blogs is known as the blogosphere.[46] Since all blogs on the Internet have the ability for its author to communicate with their audience, they may be seen as interconnected and socially networked. As a result of exploiting both the chat room and blog, terrorist's discussions in the blogosphere have the potential to influence young Islamic men here in the US in a negative way, especially if they are already down on the West.

Terrorists' Use of Search Engines

In order to find a particular blog, extremists use search engines such as Bloglines, BlogScope, and Technorati to search blog contents. Technorati, which is among the most popular blog search engines, provides current information on

[44] "Blog Issues", January 17, 2007, http://www.Internettutorials.net/engines.html, (accessed December 10, 2008)
[45] Wikipedia, Blogs, pg 2, http://en.wikipedia.org/wiki/Blog#Types, (accessed December 07, 2008)
[46]Wikipedia, Blogs, 4.

both popular searches and tags used to categorize blog postings.[47] The research community is working on going beyond simple keyword searches, by inventing new ways to navigate through huge amounts of information present in the blogosphere.[48] This is demonstrated by projects like BlogScope which as of mid-January 2009 is tracking over 31.78 million blogs with 579.86 million posts.[49]

Other ways the terrorists use Web search engines are to search for information on the World Wide Web. This information may consist of web pages, images, information and other types of files that are related to their propaganda or ideology. Some search engines also mine data available in newsbooks, databases, or open directories. Unlike Web directories, which are maintained by human editors, search engines operate algorithmically or are a mixture of algorithmic and human input.[50]

As of October 01, 2008 there were twenty-six individual search engines ranging from Alexa Web Search to Yahoo, with Google being the most popular.[51] Supplementing those were another thirty six Meta search engines, beginning with Cacti Search which provides the user with the ability to surf the web through Google, Yahoo, MSM, and Ask engines all at once and collate the results. The

[47] Welcome to Technorati, http://technoratimedia.com/about/, (accessed January 19, 2009)
[48] Michael Keren, *Blogosphere, The New Political Arena*, (Lexington Books, 2006), 73. http://www.lexingtonbooks.com/Catalog/SingleBook.shtml?command=Search&db=%5EDB/CATALOG.db&eqSKUdata=0739116711, (accessed December 10, 2008).
[49] Blogosphere research project at the University of Toronto, http://www.blogscope.net/, (accessed January 19, 2009)
[50] Wikipedia, Web search engines, http://en.wikipedia.org/wiki/Web_search_engine, (accessed December 10, 2008)
[51] "*Major Search Engines and Directories*", pg 2, http://searchenginewatch.com/2156221, (accessed October 01, 2008)

Zuula search engine provides the terrorist the opportunity to explore the web’s images and photos, news, blogs and videos from multiple search tools with separate tabs. The on-line researcher also has Searchbug, Search Engine Colossus, and Search Engine Tutorial for his collection methods.[52] The availability and free access of these Internet media platforms provide the extremists an easy way to communicate with one another and publicize propaganda efforts directed at our youth. The Internet has also become an operational security nightmare because the terrorists are accessing free, sensitive information to aid them in their planning efforts against the West.

[52] “*Major Search Engines and Directories*”, 3.

IV. The Internet is an Operational Security (OPSEC) Nightmare.

Why is maintaining OPSEC so important? Because there is so much sensitive information readily available on the Internet and both Alvin and Heidi Toffler attest to that in their non-fiction book, *War and Anti-War*, published eighteen years ago. In the reading's chapter, "Future of the Spy," the authors discuss how a web surfer and his computer hooked up to the Internet has the ability to extract all kinds of information, both classified and non-classified from Open-Source (OSINT) forums.[1] How are the terrorists exploiting OPSEC through the Internet? There is an art to collecting and analyzing friendly information for exploitable means, which our adversaries are very adept at. They approach this as trying to solve a puzzle. Intelligence collection and analysis is very much like assembling a picture puzzle. Intelligence collectors are fully aware of the importance of obtaining small bits of information (or "pieces" of a puzzle) from many different web sources and assembling them to form the overall picture. The information may be collected by monitoring e-mails, blogs, personal Web sites, or chat rooms. The premise of OPSEC in this case is that the accumulation of one or more elements of sensitive/unclassified information could reveal enough data for the terrorists to easily target our soldiers. It would be appropriate here to highlight the goal of OPSEC, as a "countermeasures" program, by denying adversary pieces of the intelligence puzzle. [2]

[1] Alvin and Heidi Toffler, *War and Anti-War: Future of the Spy* (New York: Warner Books, 1991), 191.

[2] OPSEC, "How to Solve the Puzzle", http://www.sed.monmouth.army.mil/114/isac/opsec-2.htm, (accessed December 05 ,2008)

Five-Step Process

OPSEC involves a five step process which must be followed from the first step through the last in order to be successful. The five steps are listed below and briefly explained:

Step One: Identifying critical information. Basic to the OPSEC process is determining what information, if available to one or more adversaries would harm an organization's ability to, carry out effectively, the operation or activity. This critical information constitutes the "core secrets" of the organization, i.e., the few nuggets of information that are central to the organization's mission or the specific activity. Critical information usually is, or should be, classified or at least protected as sensitive unclassified information.[3]

Step Two: Analysis of the threats. Knowing who the adversaries are and what information they require to meet their objectives is essential in determining what information is truly critical to a friendly organization's mission effectiveness. In any given situation, there is likely to be more than one adversary and each may be interested in different types of information. The adversary's ability to collect, process, analyze, and use information, i.e., the threat, must also be determined.[4]

[3] OPSEC, "*The Five Step Process*", http://www.sed.monmouth.army.mil/114/isac/fivestep.htm, (accessed December 05 ,2008)

[4] "*The Five Step Process*", Step Two, 2.

Step Three: Analysis of the vulnerabilities.   Determining the

organization's vulnerabilities involves systems analysis of how it conducts operations or activities. The organization and the activity must be viewed as the adversaries will view it, thereby providing the basis for understanding how the organization really operates and what are the true, rather than the hypothetical, vulnerabilities.[5]

Step Four: Assessment of the risks. Vulnerabilities and specific threats must be matched. Where the vulnerabilities are great and the enemy threat is evident, the risk of adversary exploitation is expected. Therefore, a high priority for protection needs to be assigned and corrective action taken. Where the vulnerability is slight and the adversary has a marginal collection capability, the priority should be low.[6]

Step Five: Application of the countermeasures. Countermeasures need to be developed that eliminate the vulnerabilities, threats, or utility of the information to the adversaries. The possible countermeasures should include alternatives that may vary in effectiveness, feasibility, and cost. Countermeasures may include anything that is likely to work in a particular situation. The decision of whether to implement countermeasures must be based on cost/benefit analysis and an evaluation of the overall program objectives.[7]

[5] "*The Five Step Process"*, Step Three, 3.
[6] "*The Five Step Process"*, Step Four, 4.
[7] "*The Five Step Process"*, Step Five, 4.

The OPSEC process must be tailored to the specific organization and activity being analyzed. Most importantly, the process is a cycle where, after countermeasures are implemented, evaluation must continue. The adversary purple dragon illustration below in Figure 7 was developed by the Joint OPSEC committee to be a reminder for anyone conveying information.

Figure 7.

The Dragon Represents the Adversary[8]

Understanding the OPSEC Process.

In order to provide a more simplified understanding of the OPSEC process, one must know the basic fundamentals. There are three guidelines to follow. First, one must understand the threat. Planners must be able to anticipate how the enemy will exploit the information domain both from the friendly and enemy perspective. Next, identify the commander's critical information so it can be protected against our adversaries. Once the information is identified, OPSEC measures will have to be followed to protect it from exploitation.[9] There are three OPSEC laws that correlate with understanding the process.

[8] The OPSEC Purple Dragon Logo, http://www.sed.monmouth.army.mil/114/isac/fivestep.htm, (accessed November 30, 2008)

[9] "OPSEC defined", http://www.sed.monmouth.army.mil/114/isac/understand.htm, (accessed December 05 ,2008)

Three Laws of OPSEC.

The first law of OPSEC understands the enemy. If you don't know the threat, how do you know what to protect? If there were no threats to DoD programs, activities, facilities, personnel, or information, there would be no need for gates, access control procedures, security clearances, and classification. However, the DoD recognizes that threats do exist--although specific threats may vary from site to site or program to program. Employees must be aware of the actual and postulated threats to DoD. In any given situation, there is likely to be more than one adversary, and each may be interested in different information.[10] Identifying what information to protect is the second law of OPSEC.

The second law of OPSEC is the next step to consider when planning. If you don't know what to protect, how do you know you are protecting it? The "what" is the critical and sensitive, or target, information that adversaries require meeting their objectives.[11] The commander should identify his critical information requirements during planning but if not the staff must draft it for him. Operational security's third law focuses on how to protect the critical information.

The third law of OPSEC is just important as the other two. An easy rule to remember is that, if commanders are not protecting their critical and sensitive information, the adversary (dragon) wins. A commander can conduct OPSEC

[10] "*The Laws of OPSEC*", pg 2, http://www.sed.monmouth.army.mil/114/isac/understand.htm, (accessed December 05 ,2008)

[11] "*The Laws of OPSEC*", 3.

vulnerability assessments, or OPSEC surveys to determine whether or not critical information is vulnerable to exploitation. An assessment is a critical analysis of "what we do" and "how we do it" from the perspective of an adversary. The evaluation will also review internal procedures and information sources to determine whether there is an inadvertent release of sensitive information.

The assessment has identified OPSEC vulnerability if the results determine that one or more critical information requirements are exploitable by an adversary. A commander must develop countermeasures to protect the information from exploitation once an OPSEC concern or vulnerability is identified.[12]

Internet OPSEC Education.

OPSEC on the Internet is such a concern for the Army that it has implemented a training program for the great number of deployed Soldiers that are using the Web as a way to keep in touch with family and friends. The root of this training began with the former Army Chief of Staff, General Peter Schoomaker's guidance for Army OPSEC training through Mobile Training Teams, who spoke to Soldiers before they deployed because the enemy was using the Internet as a tool to target them.[13] This training eventually found its way into the joint community as the Navy has also issued OPSEC Guidelines on the Internet.[14]

[12] "*The Laws of OPSEC*", 4.

[13] OPSEC MTT from 1ST IOC, Ft Belvoir, VA.

[14] US Navy Press Releases, "Maintain OPSEC Guidelines on the Internet", November 30, 2008, http://findarticles.com/p/articles, (accessed 05 December 2008)

One of the main concerns for OPSEC officials is the inadvertent release of sensitive information. This may occur through online blogging, e-mails and sensitive photographs posted on the Internet. One example of photographs was in March 2005, when three British AQ operatives were indicted by a U.S. federal court for having carried detailed reconnaissance of financial targets in lower Manhatten, Newark, New Jersey, and Washington D.C. The men were alleged to have more than 500 photographs of the sites, with most of them having been downloaded from the Internet.[15] Likewise, the Internet has numerous photos of damaged US military equipment and vehicles which the extremist are collecting and using for their battle damaged assessments.

Consequences for OPSEC Violations.

Soldiers who leak sensitive information can face serious consequences. Spc. Leonard Clark, an Arizona National Guardsman, was reduced in rank, fined $1,640.00 and sentenced to 45 days of extra duty for violating Article 92 of the UCMJ, for releasing classified information such as unit convoy routes on a Web site he ran.[16] The practice of OPSEC is such a concern because the terrorists have written a document on how to exploit all open source information found on the Internet. Al Qaeda has made extensive use of the web for intelligence-

[15] Dan Eggen, “Indictment Cites Plans to Target Financial Hubs: 3 Britons’ Extradition to Be Sought,” *Washington Post*, April 13 2005.
[16] “Blog briefing”, from the OPSEC MTT at 1st IOC, Ft. Belvoir, slide 23.

gathering purposes and targeting.[17] The illustration in figure 8 depicts the cover of the Manchester Document that was retrieved in 2002, at a terrorist's safe house in that city in England. This document was published as a guide for terrorists to carry out their jihad.[18] It explains and illustrates every possible way to kill or maim its enemies through simple means and it instructs the reader how to carry out a multitude of successful military operations. The document also explicitly advises that "openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy",[19] and lists what sensitive information the computer user should be on the lookout for while surfing the web. Information the terrorists are looking for on the Internet is: the names and photographs of important people, service members or their families, present and future military capabilities, the time and location of meetings of top government and military officials, news about U.S. diplomacy, and any significant information on U.S. military units and their positions. Not only is the Web a treasure trove of OSINT information for the jihadist, the Saudi Arabian Ministry of Interior has stated that "an 80% recruitment rate of youth by terrorist organizations is now achieved via the Internet".[20]

[17] Hoffman, Bruce of the RAND Corporation, "*Testimony- The Use of the Internet by Islamic Extremists*," presented to the House Permanent Select Committee on Intelligence (May 04, 2006): 11.

[18] The Manchester Document, http://www.globalsecurity.org/military/library/news/2005/12/mil-051202-arnews01.htm, (accessed December 05 ,2008)

[19] The Manchester Document, 3.

[20] Jane's Terrorism and Insurgency Center- Terrorists Use the Internet for Recruiting, http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e617262e70.html, (accessed January 15, 2009)

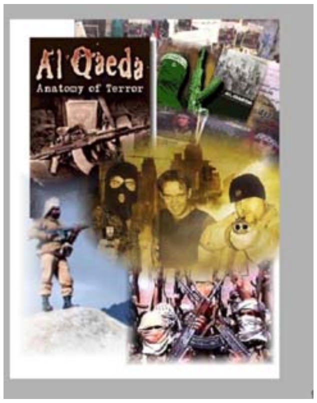


Figure 8.

The Manchester Document.[21]

V. The Making of a Potential Home-Grown Terrorist.

How Our Government is Reacting.

As already mentioned in Chapter Two, Congress recently has taken note of the Internet's power to influence potential home-grown terrorists and they are realizing that this threat is evident right here in the homeland. In particular, Senator Joseph Lieberman, who formerly was the lead for the Senate Committee on Homeland Security and Governmental Affairs said at a May 2008 press conference, "the sophisticated use of the Internet by international terror organizations and their followers is increasingly a cause of this home-grown terrorism."[22] Senator Susan Collins who is also on the committee elaborated on the concern by stating that "what makes it so troubling is we don't know how

[21] 1st IO Command Blog Briefing, "*The Manchester Document*", Illustrated

[22] The BigNews Network, "Congress: AQ Using the Internet to Recruit Terrorists in the US", pg 2, May 10, 2008, http://www.bignewsnetwork.com/forum/showthread.php107583.html, (accessed October 10, 2008)

many people are being radicalized."[23] The Committee has held five more hearings,

exploring home-grown threat assessments in the US, the European experience of domestic radicalization, and the federal government's efforts to counter the threat.[24] Mr. Robert S. Mueller, Director of the Federal Bureau of Investigation (FBI) brought this concern to senators during a Congressional Testimony in early January, 2007. During this hearing, he told the Committee stories of the FBI and other federal agencies dismantling terror groups in Georgia and Los Angeles.[25]

Noted Home-Grown Examples in the West.

The terror group of four men planning to attack the Fort Dix, New Jersey military post is another example of home-grown terrorism. Fortunately, their plans were thwarted while they were on a recon mission. Along with eyeing Fort Dix, members of the group allegedly surveyed the Lakehurst Naval Air Engineering Station and Fort Monmouth in New Jersey, Dover Air Force Base in Delaware, and a Coast Guard building in Philadelphia. They also reportedly considered an attack in conjunction with the annual Army-Navy college football game in Philadelphia.[26] In all three circumstances, the individuals were gathering terror information from the Internet for their planning needs. The Internet is

[23] The BigNews Network, "Congress: AQ Using the Internet to Recruit Terrorists in the US", 3.
[24] Majority and Minority Staff Report with Joseph Lieberman and Susan Collins, "Violent Extremism and the Internet's Influence on Home-grown Terrorists", (May 08, 2008), http://74.125.113.104/unclesam?q=cache: hvt03dwhikj:hsgac.senate.gov/public/files, (accessed October 07, 2008).
[25] FBI Congressional Testimony, "Statement Before the Senate Select Committee", January 11, 2007, http://www.fbi.gov/congress/congress07/mueller011107.htm1, (accessed October 08, 2008)
[26] Fort Dix Terror Plot Foiled "FBI: New Jersey Jihadists targeted servicemen at Army base", http://www.thesmokinggun.com/archive/years/2007/0508071ftdix1.html, (accessed January 19, 2009)

overwhelmingly connecting like-minded, jihadi web surfers in Western countries. This is evident in a recent case in Australia, where five Sydney men accused of plotting to carry out a terrorist attack allegedly collected large amounts of extremist material from the Internet that glorified violent jihad, indiscriminate mass murder and ritual beheadings.[27] These zealots have reinforced their radical notions by viewing the Internet which some Islamic extremists consider as a center of gravity.

In particular, Ayman al Zawahiri, the number two in charge of AQ knows the importance of the Internet so much that he understands it to function as a kind of virtual extremist madrassa enlisting qualified followers from around the world.[28] Some of these followers may even be here in the homeland, under the tutelage of a local mosque without the local law enforcement's knowledge. Bottom line, our government needs to be concerned with the potential threat of home-grown Islamic extremist terrorists' right here on our soil. This author's conclusion in the next chapter, offers a proposed solution that will mitigate the influence that the Internet's Islamic extremists ideology has on our youth.

[27] The Australian, On-Line Newspaper of the Year, '*Terror suspects 'planned bombings*", (November 12, 2008), http://www.theaustralian.news.com.au/story/0,25197,24639383-2702,00.html. (accessed January 19, 2009)
[28] Combating Terrorism Center at US Military Academy at West Point, "A Portal to Violent Extremism", (May 03, 2007), p.4, "Violent Extremism and the Internet's Influence on Home-grown Terrorists", (May 08, 2008), http://74.125.113.104/unclesam?q=cache: hvt03dwhikj:hsgac.senate.gov/public/files, (accessed October 07, 2008).

VI. Recommended Counter Strategy.

The solution to this threat has to be confronted in several ways. To begin with, there are three areas of concern for the counter-propaganda effort. First, the enemy's center of gravity (COG) must be understood. Secondly, the desired effects directed at the COG defined, and finally, attention needs to be focused at the counter-effort. Additionally, one must keep in mind that extremists' are generally biased towards the West, therefore, it may be future Muslim generations that offset this thinking.

The COG is so important that it must be identified and agreed upon early on when confronting this threat. Understanding the foundation of the terrorist's extremist ideology is central to its defeat. Applying the analysis of Dr. Joe Strange's "Centers of Gravity and Critical Vulnerabilities,"[1] this author argues that the extremists' ideology is the COG and the Internet is the critical capability (CC) as the vehicle to generate both force and persuasion through the extremists' propaganda, which results in home-grown terrorists. In this theory, the terrorists' influential Web sites are the critical requirements, providing the means for these propagandists to spread their hatred philosophy and finance attempts to destroy the West. These Web sites can also become critical vulnerabilities because they can be shut down once identified or countered with truthful information. Criteria for defining a COG normally consist of military and security capabilities for both the enemy and friendly forces. However, since the force applied here is through a

[1] Joe Strange, "Centers of Gravity and Critical Vulnerabilities", (Quantico, VA US Marine Corps Association, 1996), 93-96

cyber application, the armed forces are not a variable. On the contrary, security is paramount for the terrorist to remain anonymous on the Internet. Likewise, it is instrumental for our government employees and military to remain cognizant of the OPSEC factor so we do not provide classified or sensitive information unwittingly to the enemy. An effective way to do this is through reinforced DOD level organization and COCOM unit education. By doing this, it will remind our military of its responsibility to protect its critical information. Our Government employees that work on committees will have to be taught the significance of OPSEC as well.

The second are of concern, which is the desired effects of the COG must have its objectives clearly defined. Using counter-propaganda objectives to mitigate the extremist Web site's ideology ought to include clearly defined, decisive, and attainable prescribed friendly goals. In order to remedy this real threat and establish the correct goals, interest must start at the strategic level with the national leadership. After reviewing the 2000 National Security Strategy of the Clinton Administration, and the 2002 and the 2006 editions of the Bush Administration it is easy to see the disparity between the two administrations' "information" element of national power. The Clinton Security Strategy focused on the information element of national power by transmitting the strategic message to people around the world to counter misinformation and mitigate conflict. However, looking at the last two National Security Strategies under the former president, there is no reference to the importance of information as it relates to the diplomatic, military, and economic elements. Strategic communication is a powerful tool, if used in the correct manner, aimed at the right audiences, and delivering the correct message for this nation. The National Security Council, along with the State Department, needs to lead this effort, establishing the strategic policy for our nation. If the strategic communication tone is set in Washington at the outset, the DOD, the joint community, and the combatant commander will have the correct informational direction when integrating their national elements of power. Now that President Barack Obama is the Commander and Chief, hopefully the new administration will realize the potential strength and importance of information to sell our story and how it can subsequently be used to counter the Islamic extremist's ideology.

The third area of concern is important for both the government and the COCOM because it centers on a collaborative effort between counter-effort stakeholders. It is imperative that our government's counter-effort to mitigate the Internet's Islamic extremist influence be a collective one, since the AQ movement is as resilient as ever. Currently, the Department of Homeland Security (DHS) has developed an advisory council on countering terrorist acts directed against America with an attempt to synchronize the effort with the US Inter-Agency (IA) but the coordination needs some work, and unfortunately, the government's international community collaborative efforts are non-existent with the exception of a few close allies. The Federal Bureau of Investigation, Central Intelligence Agency, and the Defense Intelligence Agency are just a few of the key organizations that the DHS needs to synchronize their focus with. There are other organizations to be coordinated with as well, but they can not be mentioned in this paper because of their sensitive nature. This multi-layered coordination is very important for countering home-grown radicalization because it will synchronize law enforcement security and apprehension efforts here at home and warn of any particular cases from other countries. Subsequently, the US Government should establish a committee that involves coalition nation intelligence concerning the Internet radicalization threat directed at its youth. Once the committee is established, the coalition nations can decide on who will have the intelligence oversight depending on the nature of collection efforts. These countries could be Southeast Asia, Australia, Europe, Canada, and Japan. The point is that this committee should ensure that theses countries are coordinating their information and propaganda counter-efforts with our government too include collecting the effects of their programs.

The possibility of shutting down terrorists' web sites as soon as they appear is another counter-strategy consideration. Depending on the site, this option is not always the most intelligent thing to do because there is the potential to collect valuable information on the group sponsoring it. This information may be in the form of communication between cells, researching other terrorists' hyper-linked sites, and who is supporting the web page through finances and dialogue. Also, shutting down a terrorist Web site only temporarily disrupts their effort. To truly halt a terrorist site, the webmaster that is the controlling authority of the page must be stopped.

The Search for International Terrorists' Entities (SITE) institute which is the most famous private sector monitor of terrorist web sites supports the concern for not shutting down the sites. The SITE institute once formally a nonprofit organization has now moved to the SITE Intelligence Group,[2] a for-profit entity and this author recommends that the DHS financially support the SITE. Then the DHS can gather and analyze the SITE's collected data on terrorist web sites while creating their own database. The point here is that our government needs to work with the private sector in their attempts to counter this Internet extremist threat. Aside from the SITE institute, there are contractors for hire that will assist in constructing cyber threat data bases and analyzing threat categories.

One final point is that our Internet extremists' propaganda counter-efforts have to be measured for their effectiveness. A sample metrics diagram is below in Figure 9 for a study group's use. The framework for this model has two implied understandings. First and most important, there is an emphasis on facilitating valid, strategic, and government focused counter-messages directed against extremists' ideologies. Secondly, counter-ideology campaigns are established through the appropriate intelligence and information components that are synchronized with international coalition forces cooperation.

In the first column, the committee has to identify the extremists' Web site that will be observed. The second column takes in to account the selected purview of the site's context. The third column identifies the number of times that the page has been visited in one week but what is difficult is identifying who exactly is visiting. Column four displays which stakeholder is responsible for developing the counter message. Key here is also to promote the US message of

[2] SITE Intelligence Group located at www.siteintelgroup. (accessed December 06, 2008)

"life, liberty, and the pursuit of happiness." Column five counts the number of times the site has been visited or revisited the following week. Column six attempts to measure the effect of the counter message through assessing the number of times the site has been hit between column three and column five.

Web site visited	Ideology scope/activity of site	# Of weekly visitors to that site?	Counter-Web site/counter-propaganda effort?	# Of weekly visits after counter efforts/ response?	Assessment
GIMF	Propaganda Media conduit	100 posts to message	NCTC/West Point CT Center	125 posts to message	↑ **25%**
IAI	Militant	200 hits	MNF-I/MNC-I	198 hits	↔ **.99%**
AI	Militant	150 hits	MNF-I/MNC-I	75 hits	↓ **50%**

Figure 9.

Analyzing the Counter-Propaganda Effects on Extremists' Web Sites

Assessing the impact of the collation constructed counter-ideological messages is important for understanding their effect and intended consequences. Capturing the number of times the Web sites have been visited before and after counter-propaganda efforts on a weekly basis is paramount. The difference between the two will provide a sensing of how well the counter-strategy is working. On average, if the web site is visited less after the counter message is posted, its content should be re-evaluated. Conducting host nation polling will reinforce the assessment results.

VII. Conclusion.

This thesis attempted to validate two assumptions concerning AQ and its Islamic extremists' followers and their use of the Internet. The first assumption is that these terrorists are exploiting the Internet in order to promote their fanatical ideology. This second assumption is a result of the first, which is due to Internet exploitation, the jihadists are developing home grown terrorist youth in the West and in some cases right here in America. The paper has endeavored to show the reader how significant the use of the Internet has been for the Islamic extremists.

These terrorists used the Internet prior to 9/11 in order to facilitate the attacks on our homeland. They continue to exploit the Web today in order to spread their propaganda against the West, communicate attack plans with one another, solicit the finances to fund their operations, and gather valuable information on our government, infrastructure, and military. The five different case studies on these Web sites provide proof of how the extremists are manipulating this cyber tool to attack our civilians and military. Several examples of home grown terrorists influenced by the Internet, who have already been captured here in the homeland reinforce the second assumption. What is not known is the number of those youth that are currently being influenced here in the homeland. With the advent of cyber social networking and its multitude of personal sites on the Web, this is very difficult to measure.

Operational security for protecting valuable information is an area of concern for the Internet as well. These extremists are continuously monitoring the Web in order to obtain sensitive information so they can use it for their planning purposes. Much of this information is errantly placed on the Internet by our governmental employees and military because they are not educated in this area. Given all the information provided by this thesis on the very real threat posed by extremists' exploitation of the Internet, one can only hope the government will take appropriate measures to end their information exploitation.

Bibliography

Books

Hoffman, Bruce of the RAND Corporation, "*Testimony- The Use of the Internet by Islamic Extremists*," presented to the House Permanent Select Committee on Intel (May 04, 2006): 4.

Samuel Griffith, Sun Tzu: The Art of War (New York: Oxford University Press, 1971), 84

E. Leigh Aemstead and Dr. Maura Conway. Information Warfare, Separating Hype From Reality: Cyberterrorism, Hype and Reality, (Virginia, Potomac Books, 2007), 94

Alvin and Heidi Toffler, *War and Anti-War: Future of the Spy* (New York: Warner Books, 1991), 191

Articles

Weimann, Gabriel "Terror on the Internet: The New Agenda, The New Challenges," Seminar held at the United States Institute of Peace, Washington D.C., April 10, 2006.

The 9/11Commission Report, p.145, released 22 July 2004

Jane's Terrorism and Insurgency Center, Information Campaigns, pg 7

Acosta, David A., MAJ "Hezbollah: Deception in the 2006 Summer War", *IO Sphere*, Winter 2008, 19-23.

Shoresh, "*International Fellowship of Christians and Jews*", October 2008 Vol 14, No. 10, 3.

Department of Justice Press Conference, Subject: Federal Indictment of American Terror Suspect Adam Gadahn, (October 11, 2006), Open-file report, Dept of Justice (Wash DC 2006).

Benjamin R. Davis, The Catholic University of America CommLaw Conspectus, *"Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet"* (Fall 2006):14.

Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace", *Alleged Terror Hackers Arrested* (July 2005):2.

9/11 Commission Report, "*National Commission on Terrorist Attacks Directed Against the US*", pg 5, (May 2006), Open-file report, USIP (Wash DC March 2006).

Strange, Joe "Centers of Gravity and Critical Vulnerabilities", (Quantico, VA US Marine Corps Association, 1996), 93-96

The BigNews Network, "Congress: AQ Using the Internet to Recruit Terrorists in the US", 3.

Electronic Sources

The Moderate Voice, Secretary Gates: "Al Qaeda is better at communicating its message on the Internet than America, November 27, 2007: as quoted by NY Times", http://www.lexisnexis.com/us/lnacademic/frame.do?tokenKey=rsh-0.87603.3513028242.html

U.S Dept of State, released by the Office of the Coord for CT. "Country Reports on Terrorism, April 28, 2006", http://www.state.gov/s/ct/rls/crt/2005/64333.htm (accessed October 7, 2008

Periodical, Jane's review, 01 Nov 2001, "What the Investigation Reveals", http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed 14 Sep 2008)

Conway, Mauara "Reality Bytes," *Cyberterrorism and Terrorist Use of the Internet" (July 2005):5.* http//www.firstmonday.org/ISSUES/issue7-11/conway.html (accessed 10 October 2008)

Capital Hill Hearing Testimony, "Internet and Terrorism", 6 Nov 2007, http://psidonline.isr.umich.edu/Publications/Congressional_Testimony.pdf, (accessed 26 Sep 2008)

"How Terrorists Use the Internet": 7.62mm Justice, by Howard Salter and quoted from Gabraen, 05 Nov 2007, http://762justice.com/2007/11/05/how-terrorists-use-the-internet/, (accessed 30 Aug 2008)

U.S DOS Fact Sheet, Office of Counterterrorism- October 11, 2005, Foreign Terrorist Organizations (FTOs), http://www.state.gov/s/ct/rls/fs/37191.html (accessed October 27, 2008)

U.S DOS Chronology, The Office of the Coordinator for Counterterrorism- December 31, 2001, Identified Terrorist Groups, http://www.state.gov/s/ct/rls/fs/2001/6531.html (accessed October 7, 2008)

The Jawa Report, "The Threat of Home-grown Terrorists is Real", 6 Feb 2008, http://mypetjawa.mu.nu/archives/191108.php, (accessed 29 Sep 2008)

Washington Post, "Terrorists at the Threshold of Using Internet as Tool of Bloodshed", June

27, 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html, (accessed 26 Sep 2008)

Jane’s Terrorism and Insurgency Center, Information Campaigns, pg 6- August 01, 2007, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)

NewsFactor Network- “How the Terrorists Use the Internet”, by Matthew Devost from the Terrorist Research Center)- 12 sep 2001, http://www.newsfactor.com/perl/story/7731.html, (accessed 14 September 2008)

Al Qaeda Beats the Odds; Terror Network Uses the Gambling Web sites to Launder Money in Internet Campaign”, January 03, 209”. Report delivered by The Gazette (Montreal). http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.234911.506682717.html (accessed January 13, 2009)

The New York Times Sunday Late Edition. “The Toughest Q’s Answered in the Briefest Tweets”; January 04, 2009. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.852026074972280.html (accessed January 05, 2009)

The VNUNET.COM. “Gaza Conflict Mirrored Online”; January 03, 2009. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh- 20.646386.3489934341.html (accessed January 05, 2009)

Wikipedia, Social Networking, http://en.wikipedia.org/wiki/Social_networking, (accessed December 10, 2008)

NBC News Transcript, “Potential Terrorists Waging Jihad via the Internet”, Aug 22, 2007, http://www.jihadwatch.org/archives/2007_11.php, (accessed Oct 10, 2008)

America.gov- Dept of State. “President Bush Calls for Firm Resolve Against Terrorism, 6 October 2005” http://www.america.gov/st/washfile-english/2005/October/20051006113103adynned0.565.html (accessed October 7, 2008)

Jane’s Terrorism and Insurgency Center 2005, Information Campaigns, pg 3- March 18,2004, http://www8.janes.com/JDIC/JTIC/document View.do?docID=/content1/janesdata/magsjtic.html, (accessed 23 December, 2008)

Jihad Online: Islamic Terrorists and the Internet Org http://www.adl.org/internet/jihad.asp (accessed January 06, 2009)

Rita Katz & Josh Devon at www.jihad.com, E-Groups abused by jihadists, http://www.adl.org/internet/jihad.asp (accessed January 06, 2009)

The Enemy Within: Where Are the Islamist/Jihadist Web sites Hosted- MEMRI, and What

Can Be Done About It? Org http://memri.org/bin/latestnews.cgi?ID=IA37407#_edn6 (accessed January 06, 2009)

Pak Jihadi groups recruiting young children for Jihad, suicide attacks: MQM. Org http://in.news.yahoo.com/139/20090117/874/twl-pak-jihadi-groups-recruiting-young-c.html (accessed January 17, 2009)

Discover True Islam at Free Minds. Org http://www.free-minds.org/taxonomy/term/8 (accessed December 7, 2008)

The Globe and the Mail (Canada). "A Media-Distribution Enterprise for Global Terror, May 22, 2008". International News; Global Islamic Front. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

The Jawa Report. "Two More German GIMF Online Jihadis Arrested, November 25, 2008". Report delivered by Newstex. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.413091782222758.html (accessed December 1, 2008)

BBC Monitoring Europe – Political Supplied by BBC Worldwide Monitoring. "Islamist Arrested in Austria Was Head of German GIMF – Web site, September 13, 2007". Excerpt from report by German Spiegel Online Web site on September 12, 2007. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.928283724260083.html (accessed December 1, 2008)

Spiegel Online International. "*Al-Qaida's German Blog*", pg 2 http://www.spiegel.de/international/0,1518,434404,00.html (accessed December 15, 2008)

The New Yorker. "Azzam the American; The Making of an AQ Homeowner"; January 22, 2007. http://www.lexisnexis.com/us/lnacademia/framedo?tokenKey=rsh-20.542359.850258951.html (accessed December 01, 2008)

Al Manar Television, http://www.manartv.comlb/NewsSite/News.aspx?language, pg 2, (accessed November 15, 2008)

The Investigative Project on Terrorism, pg 2, December 03, 2008: Articles by IPT http://www.webnet.jfsc.ndu.edu/+csco+0h7567676333a2f2f6a6a6a382e776e6172662e70.html (accessed December 17, 2008)

CNN World.com, Al-Jazeera Turns its Signal West, 4 July 2005, OSINT, http://web.archive.org/web/20050710010536/http://www.cnn.com2005/world/meast (accessed 28 October 2008).

National Counter Terrorism Center, 2008 Counter Terrorism- Ansar Al Sunna, http://www.nctc.gov/site/groups/as.html, (accessed October 29, 2008)

Juba Sniper Full 15 Minutes in Baghdad", pg 1, http://video.google.com/videoplay?docid=-8302187367555388286, (accessed October 1, 2008)

OPSEC, "*The Five Step Process*", http://www.sed.monmouth.army.mil/114/isac/fivestep.htm, (accessed December 05 ,2008)

The Manchester Document, http://www.globalsecurity.org/military/library/news/2005/12/mil-051202-arnews01.htm, (accessed December 05 ,2008)

Jane's Terrorism and Insurgency Center, Information Campaigns, pg 6- August 01, 2007, http://www.webnet.jfsc.ndu.edu/+csco+0h756767633a2f2f6a6a6a382e776e617262e70.html, (accessed September 14, 2008)

Public Documents

Report source 8 May 2008, United States Senate Committee on Homeland Security and Governmental Affairs

Final Report of the National Commission on Terrorist Attacks Upon the United States. The *9/11 Commission Report: Authorized Edition* (New York & London, W.W. Norton & Company, 2004), pp. 157, 164, & 495.

United States Institute of Peace, Special Report of How Modern Terrorism Uses the Internet by Gabriel Weimann (March 2004), Open-file report, USIP (Wash DC March 2006).

Vita

Lieutenant Colonel Taylor is a United States Army Information operations (IO) officer with 20 commissioned years of service. He is basic branched as an Infantry officer and has held command and staff positions of responsibility in both the light and mechanized forces. His IO experience includes serving as the Commander for the 1st Battalion, 1st Information Operations Command and holding numerous IO leadership and IO staff positions. He has been deployed to Desert Shied/Storm and Intrinsic Action as an Infantryman and been deployed to Bosnia then Kuwait, Iraq, and Afghanistan on multiple rotations as an IO officer supporting various levels of command. His next assignment is with the Army staff at the Pentagon.